Universitat Oberta de Catalunya
uoc.edu

eRGPD

César Fernández García
Grado de Ingeniería Informática
Java EE

Vincenç Font Sagrista
Santi Caballé Llobet

Junio 2020

FICHA DEL TRABAJO FINAL

Título del trabajo:	*eRGPD*
Nombre del autor:	*César Fernández García*
Nombre del consultor:	*Vicenç Font Sagrista*
Nombre del PRA:	*Santi Caballé Llobet*
Fecha de entrega:	06/2020
Titulación:	*Grado de Ingeniería Informática*
Área del Trabajo Final:	*Java EE*
Idioma del trabajo:	*Castellano*
Palabras clave:	*RGPD, J2EE, Firma Electrónica, XMLDSig*

Resumen del Trabajo:

El sistema de información eRGPD tendrá como finalidad aportar un aplicativo que pueda ser instalado en cualquier organización cuyos sistemas de información traten datos personales y garantice el cumplimiento de la Ley Orgánica 3/2018 en relación a los nuevos derechos establecidos por el Reglamento Europeo 2016/679 (RGPD) por parte del interesado.

Dado que los requisitos funcionales se corresponden con los distintos derechos que recoge la nueva ley de protección de datos y no son dependientes de la decisión cambiante de ningún cliente, a lo que hay que añadir que tenemos un calendario fijado de antemano, se enfoca el proyecto con una metodología clásica en cascada.

El resultado es una aplicación J2EE totalmente funcional que dependiendo del nivel de integración con los distintos sistemas de información de la organización, tramitará las solicitudes de manera síncrona o asíncrona. Al tratar datos personales, la seguridad del sistema es un factor clave para el éxito del proyecto, el interesado se autenticará en el sistema con su certificado personal, y firmará electrónicamente las solicitudes que presente garantizando así la autenticidad, integridad y no repudio de éstas.

Para concluir, creo haber abordado un proyecto interesante, que resuelve una necesidad real introducida en el nuevo Reglamento de Protección de Datos, y por lo tanto de obligado cumplimiento que resulta de gran utilidad.

Abstract:

eRGPD information system will aim to provide an application that can be installed in any organization whose information systems process personal data and guarantee compliance with Organic Law 3/2018 in relation to the new rights established by the European Regulation 2016/679 (GDPR) by citizens.

Because the functional requirements correspond to the different rights included in the new data protection law and are not dependent on the changing decision of any client, and we also have a schedule set beforehand, the project is approached with a classical methodology cascading.

The result is a fully functional J2EE application, which, depending on the level of integration with the organization's information systems, will process the requests synchronously or asynchronously. When processing personal data, security is a key factor for the success of the project, the data subjects will authenticate themselves in the system with their personal certificate, and digitally sign the requests that they present, thus guaranteeing their authenticity, integrity and non-repudiation.

To conclude, in my opinion I have faced an interesting project, which solves a need introduced in the new Data Protection Regulation and, therefore, of mandatory compliance that would be very useful.

Índice

Lista de figuras

1. Introducción

1.1 Contexto y justificación del Trabajo

El 6 de diciembre de 2018 se publicó en el BOE la nueva Ley Orgánica 3/2018 de Protección de Datos Personales y Garantía de los Derechos Digitales, entrando en vigor de manera inmediata al día siguiente de su publicación. Esta ley adapta el Reglamento General de Protección de Datos europeo (RGPD) al ámbito nacional.

Esta ley establece las obligaciones de las empresas sobre cómo proceder con la información personal, los derechos que asisten a usuarios y consumidores, así como el régimen sancionador, que dependiendo del tipo de infracción fija la cuantía de las sanciones, pudiendo éstas alcanzar entre 10 y 20 millones de euros, o entre el 2% y el 4% del volumen del negocio anual global.

Finalmente, el RGPD establece en su artículo 59 que el responsable del tratamiento debe proporcionar medios electrónicos para presentar las solicitudes en el ejercicio de sus derechos en calidad de interesado, en particular cuando los datos personales se tratan por estos medios. Así como dar respuesta también por medios electrónicos si la solicitud es realizada a través de los mismos. Nuestro sistema de información, en adelante eRGPD, quiere dar respuesta a esta necesidad, aportando una solución que se integre fácilmente con los sistemas informáticos existentes en cualquier organización.

1.2 Objetivos del Trabajo

El sistema de información eRGPD tendrá como principal objetivo aportar un aplicativo que pueda ser instalado en cualquier organización cuyos sistemas de información traten datos personales y garantice el cumplimiento de la normativa legal en relación a los nuevos derechos establecidos por el Reglamento Europeo 2016/679 (RGPD) otorgados a los interesados. Dichos derechos son:

1. Derecho de acceso: Conocer si el responsable del tratamiento está o no tratando tus datos de carácter personal, y en caso afirmativo, obtener la siguiente información:
    a. Copia de mis datos personales que son objeto de tratamiento por ese responsable.
    b. Los fines del tratamiento, así como las categorías de datos personales que se traten.
    c. Los destinatarios o categorías de destinatarios a los que se han comunicado mis datos personales, o serán comunicados, incluyendo, en su caso, destinatarios en terceros u organizaciones internacionales.
    d. Información sobre las garantías adecuadas relativas a la transferencia de mis datos a un tercer país o a una organización internacional, en su caso.
    e. El plazo previsto de conservación, o de no ser posible, los criterios para determinar este plazo.
    f. Si existen decisiones automatizadas, incluyendo la elaboración de perfiles, información significativa sobre la lógica aplicada, así como la importancia y consecuencias previstas de dicho tratamiento.

    g. Si mis datos personales no se han obtenido directamente de mí, la información disponible sobre su origen.
    h. La existencia del derecho a solicitar la rectificación, supresión o limitación del tratamiento de mis datos personales, o a oponerme a dicho tratamiento.
    i. El derecho a presentar una reclamación ante una autoridad de control.

2. Derecho de rectificación: Rectificar datos personales que sean inexactos o incompletos. Se deberá aportar documentación que lo acredite al responsable del tratamiento.
3. Derecho de oposición: oponerse a que el responsable realice el tratamiento de tus datos personales en base a 2 supuestos:
    a. Tratamiento basado en una misión de interés público o en el interés legitimo.
    b. Tratamiento con finalidad mercadotecnia directa.
4. Derecho de supresión ("al olvido"): eliminación y fin del tratamiento de tus datos.
5. Derecho a la limitación del tratamiento: solicitar la suspensión del tratamiento cuando has impugnado la exactitud de tus datos (ejercido el derecho de rectificación) o cuanto te has opuesto al tratamiento mientras el responsable verifica tales hechos.
6. Derecho a la portabilidad: cuando el tratamiento se realice por medios automatizados, obtener tus datos en formato estructurado, de lectura mecánica e interoperable, y puedas transmitirlo a otro responsable del tratamiento siempre que se legitime en base al consentimiento o en el marco de la ejecución de un contrato.
7. Derecho a no ser objeto de decisiones individuales automatizadas: no ser objeto de una decisión basada únicamente en el tratamiento de tus datos, incluida la elaboración de perfiles, garantizando tu derecho a la intervención humana, expresar tu punto de vista e impugnar la decisión.

1.2.1 Alcance

El sistema de información eRGPD dispondrá de distintos modos de funcionamiento configurables, en función del grado de integración con cada uno de los sistemas de información de la organización que realicen tratamiento de datos de carácter personal:

1. Funcionamiento asíncrono: se comporta como un buzón de solicitudes, el interesado ejerce sus derechos que son registrados. Posteriormente, los encargados del tratamiento (tramitadores) atenderán las peticiones en el tiempo establecido por la ley.
2. Funcionamiento síncrono: el interesado ejerce el derecho causando un efecto inmediato. Requiere un mayor grado de integración entre nuestra aplicación y los sistemas de información de la organización. Se diseñará un servicio web (wsdl) con operaciones para cada uno de los derechos descritos. Los distintos sistemas de información que realicen tratamientos de datos de carácter personal deberán implementar dicho servicio para poder invocarlos desde nuestra aplicación.

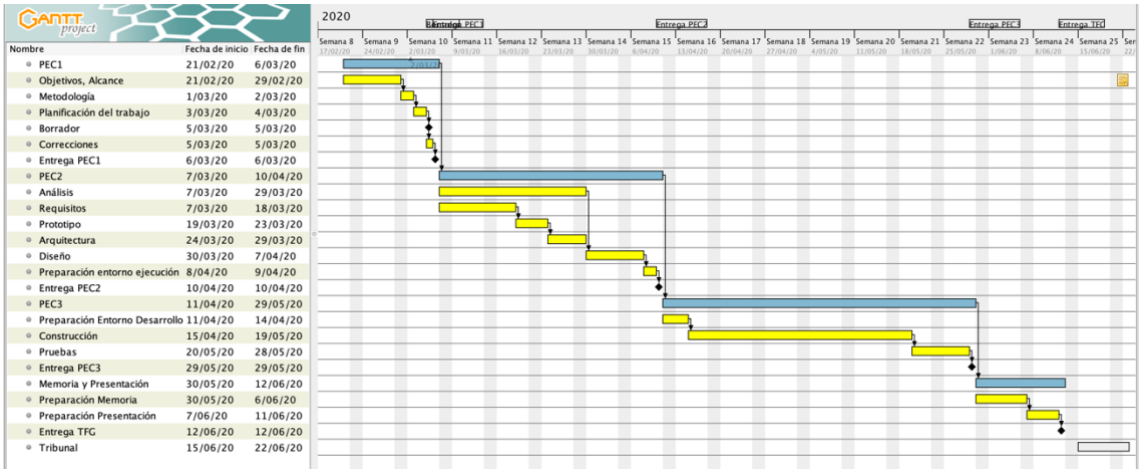
1.3 Enfoque y método seguido

Se decide enfocar el desarrollo del sistema eRGPD con una metodología clásica en cascada. Los requisitos funcionales que satisface el sistema a desarrollar están claramente definidos ya que se corresponden con los distintos derechos de los interesados que recoge el RGPD, por lo que no dependemos de las decisiones cambiantes de ningún cliente. Además, tenemos un calendario de entregas fijo de

antemano al que nos tenemos que ajustar. En resumen, sabemos lo que queremos y necesitamos, y tenemos un calendario fijo o difícil de modificar, dos motivos claves para decantarnos por esta metodología.

1.4 Planificación del Trabajo

Definimos el plan de Trabajo ajustándonos al calendario de PEC's del plan docente.



Nombre	Fecha de inicio	Fecha de fin
PEC1	21/02/20	6/03/20
Objetivos, Alcance	21/02/20	29/02/20
Metodología	1/03/20	2/03/20
Planificación del trabajo	3/03/20	4/03/20
Borrador	5/03/20	5/03/20
Correcciones	5/03/20	5/03/20
Entrega PEC1	6/03/20	6/03/20
PEC2	7/03/20	10/04/20
Análisis	7/03/20	29/03/20
Requisitos	7/03/20	18/03/20
Prototipo	19/03/20	23/03/20
Arquitectura	24/03/20	29/03/20
Diseño	30/03/20	7/04/20
Preparación entorno ejecución	8/04/20	9/04/20
Entrega PEC2	10/04/20	10/04/20
PEC3	11/04/20	29/05/20
Preparación Entorno Desarrollo	11/04/20	14/04/20
Construcción	15/04/20	19/05/20
Pruebas	20/05/20	28/05/20
Entrega PEC3	29/05/20	29/05/20
Memoria y Presentación	30/05/20	12/06/20
Preparación Memoria	30/05/20	6/06/20
Preparación Presentación	7/06/20	11/06/20
Entrega TFG	12/06/20	12/06/20
Tribunal	15/06/20	22/06/20

Figura 1. Diagrama de Gantt

1.5 Breve sumario de productos obtenidos

Se implementará un sistema de información eRGPD, junto con su documentación de análisis y diseño. En concreto se obtendrán los siguientes productos:

- La memoria del TFG:
  - Análisis y diseño
  - Especificaciones de implantación.
- Presentación y demo.
- Código Fuente del sistema eRGPD.
- Pruebas de integración automatizadas.

1.6 Breve descripción de los otros capítulos de la memoria

Los capítulos que se elaborarán a lo largo de la memoria del TFG son los siguientes:

- Análisis. Especificación del sistema eRGPD. Elaboración de un catálogo de requisitos detallado, que permita describir con precisión el sistema de información a desarrollar, y que además sirva de base para comprobar que la especificación de los modelos obtenidos es completa, y desarrollar el posterior diseño del sistema. Esta especificación contempla:
  - Especificación de requisitos.
  - Casos de uso.
  - Modelo de clases de análisis.
  - Modelo de datos.
  - Definición prototipo interfaz de usuario.

- Diseño. Elaboración de la arquitectura del sistema y sus módulos mediante diagramas de Componentes.
    - Diagrama de Arquitectura
    - Diagramas de componentes de los distintos módulos.
    - Establecimiento del entorno tecnológico y requisitos de construcción e implantación.

- Construcción. Se definen los elementos necesarios para la generación del código del sistema de información.

- Pruebas. Diseño de Pruebas unitarias y de integración automatizadas con el framework Arquillian.

- Conclusiones.

- Glosario.

- Bibliografía.

- Anexos:

    - Instrucciones de instalación y configuración.
    - Descriptor del servicio web eRGPD (WSDL)

2. Análisis

2.1 Actores

El sistema eRGPD interactúa con los siguientes actores.

2.1.1 Principales (o primarios)

Administrador

Usuario del sistema encargado de la configuración y mantenimiento de los sistemas de información que gestiona eRGPD. Registrará a los usuarios (Administrador, Responsable y Tramitador) en el sistema.

Responsable

Responsable del tratamiento/sistema de información (figura recogida en el RGPD). Podrá serlo de uno o varios sistemas de información.

Tramitador

Encargado en un determinado sistema de información de la tramitación asíncrona de las solicitudes presentadas.

Solicitante

Interesado que ejerce derecho recogido en RGPD sobre un sistema de información.

2.1.2 De apoyo (o secundarios)

Sistema de información

Sistema de información de la organización que gestiona datos de carácter personal sobre el que el solicitante ejerce un derecho.

Autofirma

Aplicación de escritorio que le permite al solicitante firmar electrónicamente con su certificado personal las solicitudes que presente en el ejercicio de sus derechos.

2.1.3 Diagrama usuarios del sistema

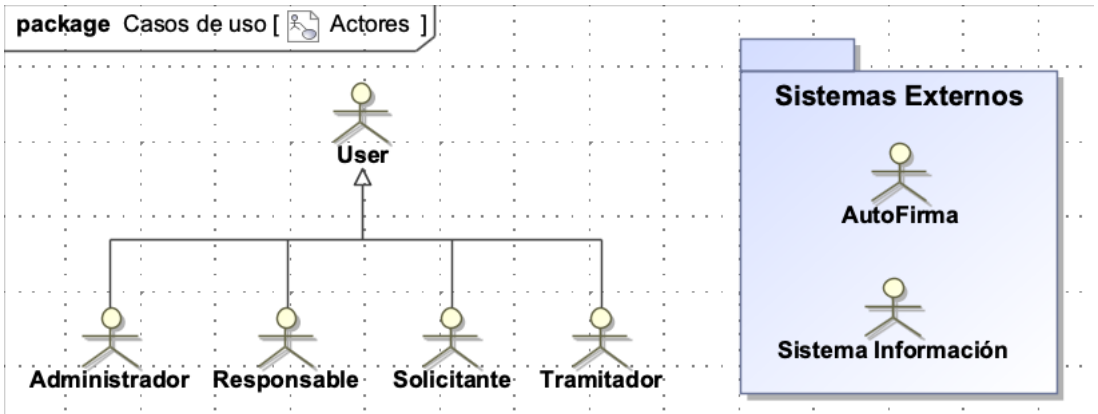


Figura 2. Actores

2.2 Requisitos

2.2.1 Requisitos Funcionales

R-001 – Gestionar Sistemas de Información

Descripción	El administrador podrá gestionar la configuración de los sistemas de información de la organización en eRGPD.
Actor	Administrador

R-002 - Gestionar usuarios y perfiles

Descripción	El administrador gestionará las cuentas de usuario de la organización, contemplando 3 perfiles: - Administrador - Responsable de tratamiento - Tramitador
Actor	Administrador

R-003 - Generar Informe Sistema de Información

Descripción	El responsable del tratamiento podrá generar un informe con estadísticas sobre los distintos sistemas de información de los que es responsable.
Actor	Responsable

R-004 - Consultar Solicitudes

Descripción	El sistema permitirá consultar las solicitudes presentadas, comprobar el estado de la tramitación, y en caso de estar resueltas, ver la resolución.
Actor	Solicitante, Tramitador

R-005 - Tramitar solicitudes

Descripción	El sistema permitirá resolver las solicitudes presentadas por los interesados, de dos modos distintos: - Síncrono. Sin intervención del tramitador produciendo una resolución en el mismo momento de la petición. Requiere un alto grado de integración con el sistema destino de la solicitud. - Asíncrono. Un tramitador del sistema de información estudiará la solicitud y la resolverá.
Actor	Tramitador (asíncrono), Sistema Información (síncrono)

R-006 - Ejercer derecho

Descripción	El interesado podrá ejercer derecho en los distintos sistemas de información que gestione eRGPD.
Actor	Solicitante

R-007 - Autenticarse en el sistema

Descripción	Dado el carácter de los datos a tratar, se requiere un alto grado de seguridad. Los usuarios tendrán que autenticarse en el sistema con su

	certificado personal. No obstante, una vez registrados en el sistema, podrán configurar en su perfil un nombre de usuario y una password para identificarse por este medio. El sistema registrará automáticamente a los solicitantes la primera vez que se autentiquen con su certificado personal. Los usuarios de la organización los registra un administrador.
Actor	Administrador, Responsable, Tramitador, Solicitante

R-008 - Firmar Solicitud

Descripción	El interesado deberá firmar con su certificado personal las solicitudes presentadas.
Actor	Solicitante, Autofirma

R-009 - Mi cuenta

Descripción	Un usuario autenticado podrá acceder a los datos de su cuenta para actualizar su perfil.
Actor	Administrador, Responsable, Tramitador, Solicitante

R-010 – Cambiar Idioma

Descripción	Un usuario podrá cambiar el idioma en el que interactuará con eRGPD.
Actor	Administrador, Responsable, Tramitador, Solicitante

2.2.2 Requisitos No Funcionales

Requisitos Operacionales

- El sistema debe ser multiplataforma, pudiéndose desplegar en distintos servidores de aplicaciones. De igual manera, los datos deben poder ser migradas a otros gestores de bases de datos.
- Los usuarios deben poder acceder a la aplicación desde cualquier navegador.

Requisitos de Seguridad

- Los datos personales de los usuarios deberán estar protegidos contra accesos no autorizados.
- La comunicación entre el navegador del usuario y el sistema eRGPD ha de ser cifrada.
- Los solicitantes deben firmar las solicitudes con su certificado personal, garantizando así la identidad del solicitante, la integridad y el no repudio de las solicitudes.
- Un solicitante solo podrá ver sus propias solicitudes.

Requisitos Legales

- El sistema debe cumplir el RGPD respecto al tratamiento de datos personales de los usuarios.

Requisitos de Usabilidad

- Internacionalización y localización. Adaptabilidad a distintos idiomas sin necesidad de hacer cambios en el código.
- El sistema en caso de error debe mostrar mensajes informativos y comprensibles por el usuario.

2.3 Casos de uso

Definimos los casos de uso del sistema y la relación con los requisitos que satisfacen, así como los actores involucrados:

ID	Caso de uso	Actores	Requisito
CU-001	Consultar Listado Sistemas de Información	Administrador	R-001
CU-002	Editar Sistema de Información	Administrador	R-001
CU-003	Habilitar/Deshabilitar Sistema de información	Administrador	R-001
CU-004	Crear Nuevo Sistema de información	Administrador	R-001
CU-005	Registrar usuario	Administrador	R-002
CU-006	Informe Sistemas de Información	Responsable	R-003
CU-007	Buscar Solicitudes	Tramitador	R-004
CU-008	Consultar solicitudes pendientes	Tramitador	R-004
CU-009	Consultar Solicitudes en Tramitación	Tramitador	R-004
CU-010	Consultar Solicitudes Resueltas	Tramitador	R-004
CU-011	Tramitar Solicitud Derecho de Acceso	Tramitador	R-005
CU-012	Tramitar Solicitud Derecho de Rectificación	Tramitador	R-005
CU-013	Tramitar Solicitud Derecho de Supresión (al olvido)	Tramitador	R-005
CU-014	Tramitar Solicitud Derecho de Oposición	Tramitador	R-005
CU-015	Tramitar Solicitud Derecho A la Portabilidad	Tramitador	R-005
CU-016	Tramitar Solicitud Derecho a la limitación del tratamiento	Tramitador	R-005
CU-017	Tramitar Solicitud Derecho A no ser objeto de decisiones individuales automatizadas	Tramitador	R-005
CU-018	Mi cuenta	Todos	R-009
CU-019	Seleccionar Sistema y Derecho	Solicitante	R-006
CU-020	Solicitar Derecho de Acceso	Solicitante	R-006
CU-021	Solicitar Derecho de Rectificación	Solicitante	R-006
CU-022	Solicitar Derecho de Supresión (al olvido)	Solicitante	R-006
CU-023	Solicitar Derecho de Oposición	Solicitante	R-006
CU-024	Solicitar Derecho A la Portabilidad	Solicitante	R-006
CU-025	Solicitar Derecho a la limitación del tratamiento	Solicitante	R-006
CU-026	Solicitar Derecho A no ser objeto de decisiones individuales automatizadas	Solicitante	R-006
CU-027	Consultar Mis solicitudes	Solicitante	R-004
CU-028	Consultar Resolución de solicitud presentada	Solicitante	R-004
CU-029	Autenticación con Certificado Personal	Todos	R-007
CU-030	Autenticación con usuario/password	Todos	R-007
CU-031	Logout	Administrador	R-007
CU-032	Firmar	Solicitante	R-008
CU-033	Cambiar Idioma	Todos	R-010

2.3.1 Diagrama de casos de uso

A continuación, por legibilidad incluyo los diagramas de casos de uso de eRGPD, organizados en paquetes.

2.3.1.1 Seguridad

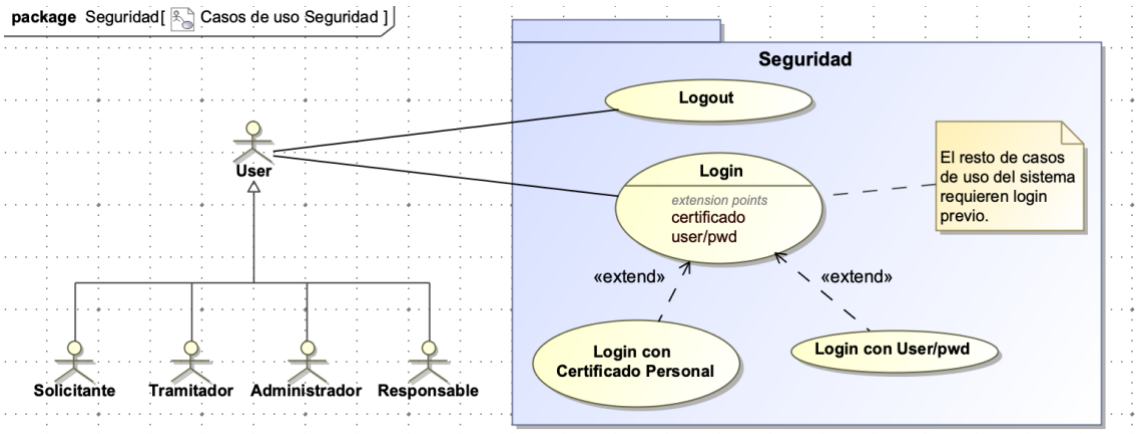


Figura 3. Diagrama de Casos de Uso – Seguridad

2.3.1.2 Administración

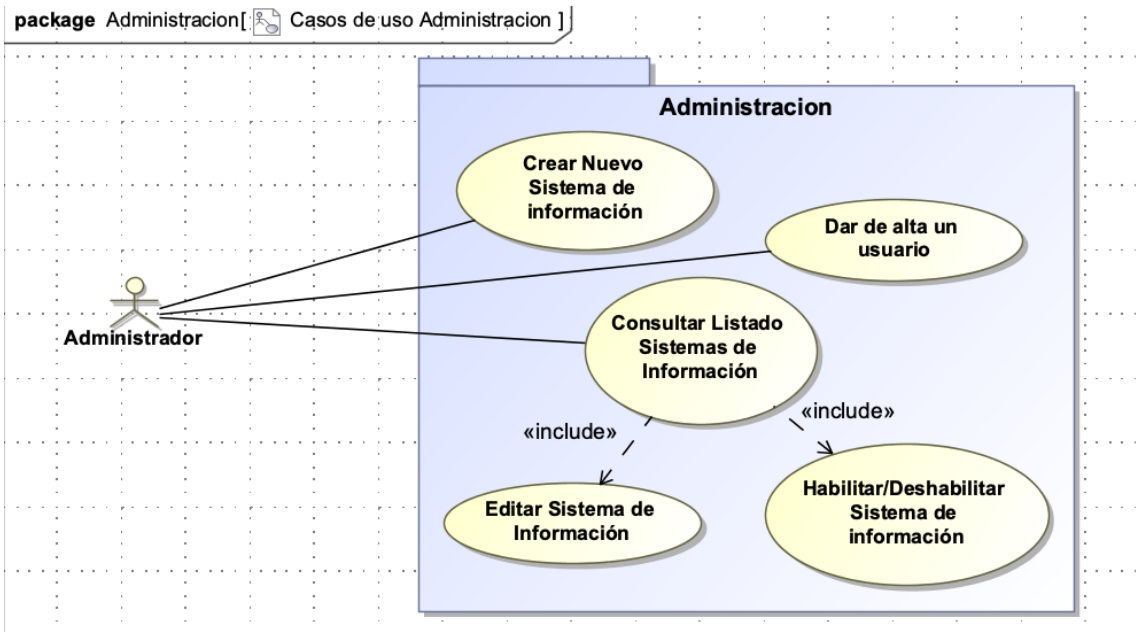


Figura 4. Diagrama de Casos de Uso – Administración

2.3.1.3 Solicitudes

Solicitante

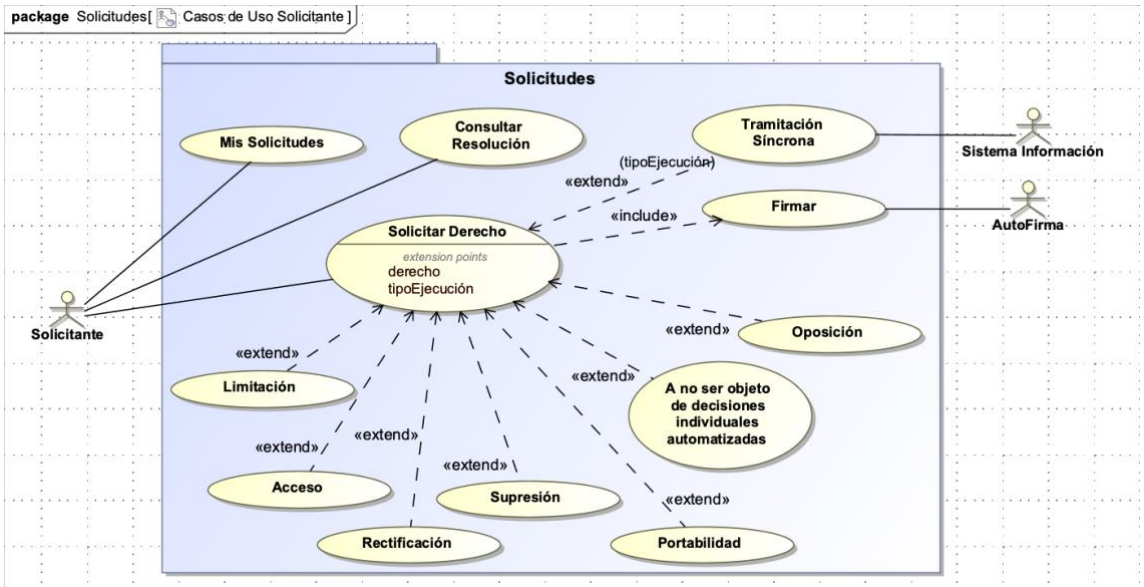


Figura 5. Diagrama de Casos de Uso – Solicitudes/Solicitante

Tramitador

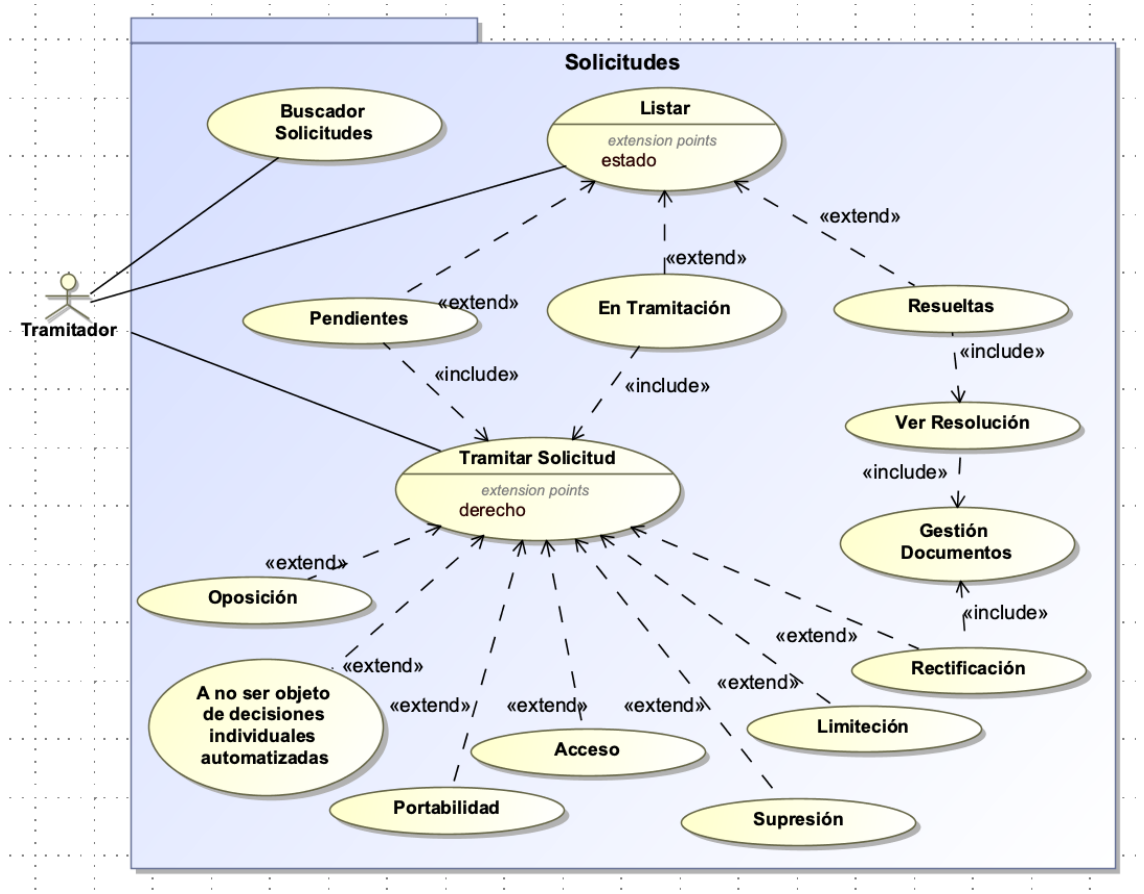


Figura 6. Diagrama de Casos de Uso – Solicitudes/Tramitador

Responsable

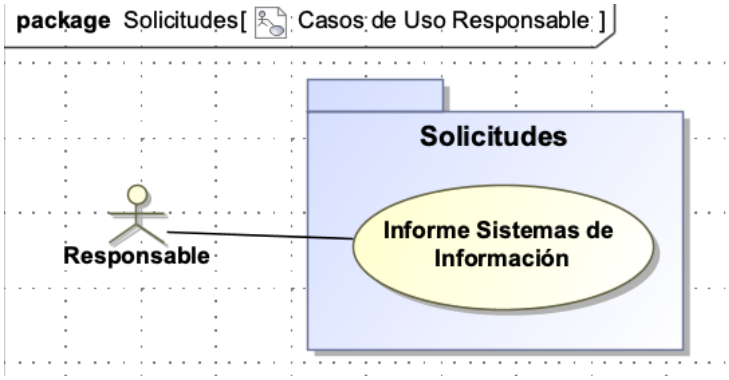


Figura 7. Diagrama de Casos de Uso – Solicitudes/Responsable

2.3.1.4 Profile

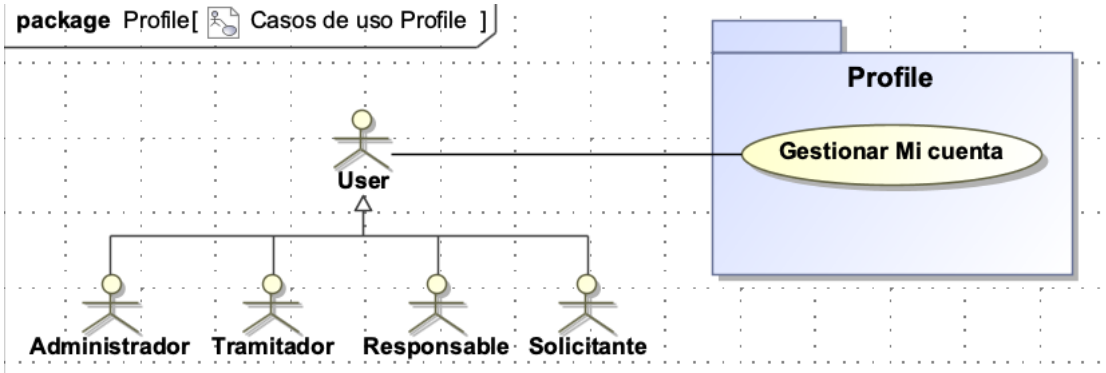


Figura 8. Diagrama de Casos de Uso – Profile

2.3.2 Descripción detallada de casos de uso

CU-001 – Consultar Listado Sistemas de Información

Descripción del caso de uso	El administrador podrá consultar un listado con los Sistemas de Información dados de alta en el sistema.
Actor(es) participante(s)	Administrador
Secuencia normal	1. El administrador selecciona la opción de menú "Sistemas de Información". 2. El sistema muestra una pantalla un listado con la información relativa a los sistemas dados de alta. Listado: - Este listado contiene las siguientes columnas: o Nombre del Sistema o Descripción del Sistema o Responsable del tratamiento o Botón de Edición o Botón de Habilitar/Deshabilitar También aparece un botón que permite dar de alta un Sistema (botón "Nuevo")
Flujo alternativo 1	1. Si no existen resultados, se muestra el listado vacío con un mensaje informativo.

Precondición	El administrador se ha logado en el sistema.
Postcondición	Se muestran los sistemas de información dados de alta.
Comentarios	Figura 48

CU-002 – Editar Sistema de Información

Descripción del caso de uso	El administrador podrá visualizar y editar los detalles del Sistema de información.
Actor(es) participante(s)	Administrador
Secuencia normal	1. El administrador pulsa en el botón de edición de un registro del listado de sistemas de información. 2. El sistema muestra un formulario con los siguientes campos: - Nombre del sistema (no editable). - Descripción del sistema. - URL Endpoint: url del web service que implementa la tramitación síncrona en el sistema. - Responsable: combo con los responsables de tratamiento dados de alta en eRGPD. - Listado de Derechos. Con las siguientes columnas: o Derecho o Tipo de Ejecución: Síncrono/Asíncrono. Aparecen 2 botones: - "Actualizar": Guarda los cambios. - "Cancelar": No guarda los cambios. 3. El administrador pulsa el botón Actualizar. Se guardan los datos del sistema de información.
Flujo Alternativo	3b. El administrador pulsa el botón Cancelar. No se guardan los cambios.
Precondición	El administrador accede a la consulta del listado de Sistemas de Información (CU-001) y pulsa en el botón "Editar" de uno determinado.
Postcondición	Se vuelve a la pantalla del listado de sistemas de información (CU-001).
Comentarios	Figura 51

CU-003 – Habilitar/Deshabilitar Sistema de información

Descripción del caso de uso	El administrador podrá habilitar y deshabilitar un sistema de información. Solo los habilitados podrán ser seleccionados (CU-019) por los interesados para presentar solicitudes.
Actor(es) participante(s)	Administrador
Secuencia normal	1. El administrador pulsa en el botón habilitar/deshabilitar del listado de los sistemas de información. 2. El botón cambiará de color (verde: habilitado, rojo: deshabilitado) en función del estado.

Precondición	El administrador accede a la consulta del listado de sistemas de información (CU-001).
Postcondición	El botón pulsado cambia de color (verde/rojo) en función de su estado actual.
Comentarios	Figura 49

CU-004 – Crear Nuevo Sistema de información

Descripción del caso de uso	El administrador podrá dar de alta nuevos sistemas de información.
Actor(es) participante(s)	Administrador
Secuencia normal	1. El administrador pulsa en el botón "Nuevo". 2. El sistema muestra un formulario con los siguientes campos: - Nombre del sistema (no editable). - Descripción del sistema. - URL Endpoint: url del web service que implementa la tramitación síncrona en el sistema. - Responsable: combo con los responsables de tratamiento dados de alta en eRGPD. - Responsable: combo con los responsables de tratamiento dados de alta. Aparecen 2 botones: - Actualizar: Guarda los cambios. - Cancelar: No guarda los cambios. 3. El administrador rellena los datos del sistema. 4. El administrador pulsa Guardar. Se crea el sistema.
Flujo alternativo 1	4b. El administrador pulsa Cancelar. No se guarda el sistema
Precondición	El administrador accede a la consulta del listado de Sistemas de Información (CU-001).
Postcondición	Se vuelve al listado de sistemas de información (CU-001), donde aparecerá el nuevo sistema.
Comentarios	Figura 50

CU-005 – Registrar usuario

Descripción del caso de uso	El administrador podrá dar de alta usuarios (Administradores, Responsables de tratamientos, Tramitadores).
Actor(es) participante(s)	Administrador
Secuencia normal	1. El administrador selecciona la opción de menú "Registrar". 2. El sistema muestra en pantalla un formulario con campos dependiendo del perfil seleccionado. Formulario: - Campos comunes:

	o Perfil: combo con las opciones: Administrador, Tramitador y Responsable. Dependiendo de la selección, aparecerán campos en el formulario específicos de ese perfil. o Número serie certificado o Usuario o NIF o Nombre y apellidos. o Email. - Campos específicos perfil Responsable: o Listado sistemas de información. Select múltiple/Checkbox para cada sistema. - Campos específicos perfil Tramitador o Sistema de información. Select simple/Combo de sistemas. Aparecen 2 botones: - "Guardar": Da de alta al usuario en el sistema. - "Cancelar": No guarda al usuario. 3. El administrador pulsa el botón Guardar.
Flujo Alternativo	3b. El administrador pulsa Cancelar.
Precondición	El administrador se ha logado en el sistema.
Postcondición	Usuario registrado en el sistema con password inicial su nombre de usuario. Si damos de alta un responsable asociándole un sistema que ya tuviera otro asociado, éste dejará de serlo en favor del nuevo dado que solo puede haber un responsable del tratamiento.
Comentarios	Figura 52

CU-006 – Informe Sistemas de Información

Descripción del caso de uso	El responsable del tratamiento podrá generar un informe con datos estadísticos de cuyos sistemas es responsable. Solicitudes pendientes de tramitar, en trámite, resueltas por sistema y por tramitador.
Actor(es) participante(s)	Responsable
Secuencia normal	1. Se pulsa la opción de menú "Informe Sistemas". 2. El sistema muestra un formulario con un combo relleno con los sistemas de información del responsable logado, y un botón Generar. 3. El responsable seleccionará un sistema de información y pulsará Generar. 4. El sistema muestra una pantalla: - Cuadro resumen del sistema: o Número total de solicitudes recibidas en estado pendiente. o Número total de solicitudes recibidas en estado tramitación (asignado a un

	tramitador). o Número total de solicitudes resueltas. - Listado de tramitadores del sistema con el total de solicitudes que están tramitando y que han resuelto.
Precondición	El usuario se ha logado en el sistema.
Postcondición	Se muestra informe en pantalla.
Comentarios	Figura 53

CU-007 – Buscar Solicitudes

Descripción del caso de uso	El tramitador podrá buscar solicitudes de su sistema de información.
Actor(es) participante(s)	Tramitador
Secuencia normal	1. El tramitador selecciona la opción de menú "Buscador de Solicitudes". 2. El sistema muestra una cabecera con campos para filtrar las solicitudes: - Derecho solicitado. - Estado: o Pendiente: solicitudes pendientes de tramitar en el sistema. o Tramitación. Solicitudes que el tramitador tiene asignada y está elaborando resolución. o Resueltas. Solicitudes que ha resuelto. 3. El tramitador selecciona filtro y pulsa botón Buscar. 4. El sistema muestra un listado con las solicitudes que cumplen el filtro. - Este listado contiene las siguientes columnas: o Nombre del Solicitante o Fecha y hora solicitud. o Derecho solicitado. o Dependiendo del estado de la solicitud, aparecerá un botón: ▪ Tramitar. Para solicitudes en estado Pendiente o en Tramitación ▪ Resolución. Para solicitudes resueltas.
Flujo alternativo 1	2b. Si no existen solicitudes, se informa.
Precondición	El tramitador se ha logado en el sistema.
Postcondición	Se muestran las solicitudes.
Comentarios	Figura 54

CU-008 – Consultar solicitudes pendientes

Descripción del caso de uso	El tramitador podrá listar las solicitudes pendientes de tramitar en su sistema de información.
Actor(es)	Tramitador

participante(s)	
Secuencia normal	1. El tramitador selecciona la opción de menú "Pendientes". 2. El sistema muestra un listado con las solicitudes pendientes de tramitar con las columnas: - Nombre del Solicitante - Fecha y hora solicitud. - Derecho solicitado. - Botón "Tramitar" (CU-011 – CU-017)
Flujo alternativo 1	2b. Si no existen resultados, se muestra el listado vacío con un mensaje informativo.
Precondición	El tramitador se ha logado en el sistema.
Postcondición	Se muestran las solicitudes.
Comentarios	Figura 55

CU-009 – Consultar Solicitudes en Tramitación

Descripción del caso de uso	El tramitador podrá listar las solicitudes que ha empezado a tramitar.
Actor(es) participante(s)	Tramitador
Secuencia normal	1. El tramitador selecciona la opción de menú "En Tramitación". 2. El sistema muestra un listado con las solicitudes que el tramitador está tramitando. - Este listado contiene las siguientes columnas: o Nombre del Solicitante o Fecha y hora solicitud. o Derecho solicitado. o Botón "Tramitar" (CU-011 – CU-017)
Flujo alternativo 1	2b. Si no existen resultados, se muestra el listado vacío con un mensaje informativo.
Precondición	El tramitador se ha logado en el sistema.
Postcondición	Se muestran las solicitudes.
Comentarios	Figura 55

CU-010 – Consultar Solicitudes Resueltas

Descripción del caso de uso	El tramitador podrá listar las solicitudes que ha resuelto.
Actor(es) participante(s)	Tramitador
Secuencia normal	1. El tramitador selecciona la opción de menú "Resueltas". 2. El sistema muestra un listado de las solicitudes que ha resuelto las siguientes columnas: o Nombre del Solicitante o Fecha y hora solicitud.

	○ Derecho solicitado. ○ Botón “Resolución”
Flujo alternativo 1	2b. Si no existen resultados, se muestra el listado vacío con un mensaje informativo.
Precondición	El tramitador se ha logado en el sistema.
Postcondición	Se muestran las solicitudes.
Comentarios	Figura 56

CU-011 – Tramitar Solicitud Derecho Acceso

Descripción del caso de uso	El tramitador podrá resolver solicitudes de acceso presentadas a su sistema de información.
Actor(es) participante(s)	Tramitador
Secuencia normal	1. El tramitador pulsa el botón “Tramitar” en el listado de solicitudes (CU-007, CU-008, CU-009) de una solicitud en estado “Pendiente” o “Tramitación”. 2. El sistema muestra el detalle de la solicitud y un formulario de tramitación: - Detalle de la solicitud: ○ Solicitante. - Formulario de tramitación con los siguientes campos: ○ Observaciones ○ Documento. Adjuntará el documento con los datos personales del solicitante. También aparecen los botones dependiendo del estado de la tramitación: - “Admitir a trámite”: El tramitador se asigna la solicitud para trabajar en ella. - “Denegada”. Resolución negativa. El sistema no está tratando los datos del solicitante. - “Aceptada”. Resolución positiva. Se adjunta a la resolución el documento de datos personales. - “Cancelar”. Se sale sin cambios.
Precondición	El tramitador se ha logado en el sistema y pulsa “Tramitar” en una solicitud no resuelta.
Postcondición	La solicitud se almacena en el sistema actualizando si estado.
Comentarios	Figura 57 (dependiente de derecho solicitado)

CU-012 – Tramitar Solicitud Derecho Rectificación

Descripción del caso de uso	El tramitador podrá tramitar solicitudes de rectificación presentadas a su sistema de información.
Actor(es) participante(s)	Tramitador
Secuencia normal	1. El tramitador pulsa el botón “Tramitar” en el listado de solicitudes (CU-007, CU-008, CU-009) de una

	solicitud en estado “Pendiente” o “Tramitación”. 2. El sistema muestra el detalle de la solicitud y un formulario de tramitación: - Detalle de la solicitud: o Solicitante. o Datos incorrectos. o Documento que lo acredita y botón para descargar el documento. - Formulario de tramitación con los siguientes campos: o Observaciones También aparecen los botones dependiendo del estado de la tramitación: - “Admitir a trámite”/”Guardar”: El tramitador se asigna/guarda la solicitud. - “Denegada”. Resolución negativa. El sistema no está tratando los datos del solicitante. - “Aceptada”. Resolución positiva. Se adjunta a la resolución el documento de datos personales. - “Cancelar”. Se sale sin cambios.
Precondición	El tramitador se ha logado en el sistema y pulsa “Tramitar” en una solicitud no resuelta.
Postcondición	La solicitud se almacena en el sistema actualizando si estado.
Comentarios	Figura 57 (dependiente de derecho solicitado)

CU-013 – Tramitar Solicitud Derecho Supresión (al olvido)

Comentarios	Ver CU-012, aplicado al derecho de supresión.

CU-014 – Tramitar Solicitud Derecho Oposición

Descripción del caso de uso	El tramitador podrá tramitar solicitudes de oposición presentadas a su sistema de información, en el caso que el tipo de ejecución de ese derecho en el sistema del tramitador sea asíncrono.
Actor(es) participante(s)	Tramitador
Secuencia normal	1. El tramitador pulsa el botón “Tramitar” en el listado de solicitudes (CU-007, CU-008, CU-009) de una solicitud en estado “Pendiente” o “Tramitación”. 2. El sistema muestra el detalle de la solicitud y un formulario de tramitación: - Detalle de la solicitud: o Solicitante. o Alega. Motivo que alega (interés público, interés legítimo o fines estadísticos). o Situación personal que acredita para oponerse al tratamiento de sus datos. - Formulario de tramitación con los siguientes

	campos: o Observaciones También aparecen los botones dependiendo del estado de la tramitación: - "Admitir a trámite"/"Guardar": El tramitador se asigna/guarda la solicitud. - "Denegada". Resolución negativa. El sistema no está tratando los datos del solicitante. - "Aceptada". Resolución positiva. Se adjunta a la resolución el documento de datos personales. - "Cancelar". Se sale sin cambios.
Precondición	El tramitador se ha logado en el sistema y pulsa "Tramitar" en una solicitud no resuelta.
Postcondición	La solicitud se almacena en el sistema actualizando si estado.
Comentarios	Figura 57 (dependiente de derecho solicitado)

CU-015 – Tramitar Solicitud Derecho Portabilidad

Descripción del caso de uso	El tramitador podrá tramitar solicitudes a la portabilidad presentadas a su sistema de información. Este derecho es una extensión del derecho de "Acceso", en el que sí es técnicamente posible, se envía al destinatario de la portabilidad los datos personales en formato estructurado del interesado. eRGPD contempla pedir el email del destino para enviar dicho documento (el envío de mail no lo contempla esta versión). En su defecto, el solicitante podrá acceder a sus datos personales consultando la resolución (como en el derecho de acceso).
Comentarios	Ver CU-011, aplicado al derecho de portabilidad.

CU-016 – Tramitar Solicitud Derecho Limitación del tratamiento.

Comentarios	Ver CU-014, aplicado al derecho de limitación. En los datos de la solicitud, aparecerá el motivo que alega (tratamiento ilícito o datos personales innecesarios).

CU-017 – Tramitar Solicitud Derecho No decisiones individuales automatizadas

Comentarios	Ver CU-012, aplicado al derecho a no ser objeto de decisiones individuales automatizadas.

CU-018 – Mi Perfil

Descripción del caso de uso	El usuario podrá ver los datos de su perfil de usuario.
Actor(es) participante(s)	Administrador, Responsable, Tramitador, Solicitante

Secuencia normal	1. El usuario pulsa en el botón "Mi Perfil" en la parte superior derecha de la página. 2. El sistema muestra un formulario con los siguientes campos de su cuenta: - Usuario y password. - Nombre y Apellidos. - email. Aparecen 2 botones: - "Actualizar": Guarda los cambios. - "Cancelar": No guarda los cambios. 3. El usuario actualiza los datos. 4. El usuario pulsa "Actualizar".
Flujo alternativo 1	2b. Error usuario ya registrado. 4b. El usuario pulsa Cancelar. No se guardan los cambios
Precondición	El usuario está logado.
Postcondición	Se vuelve a la pantalla de inicio.
Comentarios	Figura 48

CU-019 – Seleccionar Sistema y Derecho

Descripción del caso de uso	El solicitante selecciona el sistema de información y el derecho que quiere ejercer.
Actor(es) participante(s)	Solicitante
Secuencia normal	1. El solicitante pulsa en el del menú "Solicitar". 2. El sistema muestra un formulario con los siguientes campos de su cuenta: - Sistema. Combo con los sistemas de información en estado Habilitado. - Derecho. Combo con los derechos que puede ejercer contemplados en el RGPD. - Nota informativa. Aviso dependiente de la selección anterior, informando de si la respuesta va a ser síncrona o asíncrona. - Botón "Solicitar".
Precondición	Solicitante logado en el sistema
Postcondición	Dependiendo del derecho seleccionado, redirigirá a "Solicitar Derecho <Derecho>" (CU020-CU-026)
Comentarios	Figura 58

CU-020 – Solicitar Derecho Acceso

Descripción del caso de uso	El solicitante ejerce el derecho de acceso en un sistema de información, Si el sistema de información está tratando sus datos personales, deberá facilitarle en el plazo de un mes por medios electrónicos: - Copia de mis datos personales - Los fines del tratamiento, así como la categoría de

	mis datos personales. - Los destinatarios a los que se hubieran comunicado mis datos personales. - Información sobre envío a un tercer país u organización internacional. - El plazo previsto de conservación. - Si existen decisiones automatizadas, incluyendo la elaboración de perfiles. - Información disponible sobre su origen. - La existencia del derecho a solicitar la rectificación, supresión o limitación del tratamiento de mis datos personales, o a oponerme a dicho tratamiento. - El derecho a presentar una reclamación ante una autoridad de control

Actor(es) participante(s)	Solicitante
Secuencia normal	1. El solicitante el botón "Solicitar" (CU-019). 2. El sistema muestra una página 2 secciones: - Sistema: o Título: el nombre del sistema al que se presenta solicitud. o Responsable del sistema: Nombre e email. - SOLICITA: o Información sobre los datos personales que recoge el RGPD se le debe facilitar al interesado. o Botón de "Firmar y Enviar" o Botón de "Cancelar" 3. El usuario pulsa "Firmar y Enviar" (CU-032) 4. El sistema muestra un listado con sus solicitudes.
Flujo alternativo 1	3b. El solicitante pulsa "Cancelar". Se vuelve a la pantalla anterior de selección de Sistema/Derecho (CU-019)
Precondición	El solicitante dispone de certificado personal.
Postcondición	Se almacena la solicitud.
Comentarios	Figura 59 (dependiente de derecho solicitado)

CU-021 – Solicitar Derecho Rectificación

Descripción del caso de uso	El solicitante ejerce el derecho de rectificación en un sistema de información seleccionado. En la solicitud deberá constar los datos personales que sean inexactas o incompletos y la rectificación que hay que realizar, acompañando a la solicitud la documentación que lo acredite.
Actor(es) participante(s)	Solicitante
Secuencia normal	1. El solicitante el botón "Solicitar" (CU-019). 2. El sistema muestra una página 2 secciones:

	- Sistema: o Título: el nombre del sistema al que se presenta solicitud. o Responsable del sistema: Nombre e email. - SOLICITA: o Información sobre el derecho de rectificación que recoge el RGPD. o Formulario con 2 campos: ▪ Datos sobre los que solicita rectificación (text area) ▪ Botón "Seleccionar archivo" Adjunta fichero que acredita la rectificación o Botón de "Firmar y Enviar" o Botón de "Cancelar" 3. El usuario pulsa "Firmar y Enviar" (CU-032) 4. El sistema muestra un listado con sus solicitudes.
Flujo alternativo 1	3b. El solicitante pulsa "Cancelar". Se vuelve a la pantalla anterior de selección de Sistema/Derecho (CU-019)
Precondición	El solicitante dispone de certificado personal.
Postcondición	Se almacena la solicitud.
Comentarios	Figura 59 (dependiente de derecho solicitado)

CU-022 – Solicitar Derecho Supresión (al olvido)

Descripción del caso de uso	El solicitante ejerce el derecho de supresión en un sistema de información. Se le deberá notificar el resultado de la supresión. En caso de que se acuerde no suprimir total o parcialmente sus datos personales, se le comunique motivadamente a fin de reclamar ante la autoridad de control correspondiente (AEPD).
Comentarios	Ver CU-020, aplicado al derecho de supresión.

CU-023 – Solicitar Derecho Oposición

Descripción del caso de uso	El solicitante ejerce el derecho de oposición en un sistema de información. Deberá motivar la solicitud por uno de los siguientes supuestos: - El tratamiento se basa en una misión de interés público. - El tratamiento se basa en la satisfacción de intereses legítimos. - El tratamiento se está realizando con fines de investigación científica o histórica o fines estadísticos. E informar situación personal para oponerse al tratamiento sin perjuicio de que corresponde al responsable acreditar motivos legítimos que prevalezcan sobre mis intereses.
Comentarios	Ver CU-020, aplicado al derecho de oposición.

CU-024 – Solicitar Derecho Portabilidad.

Descripción del caso de uso	El solicitante ejerce el derecho a la portabilidad en un sistema de información. Consiste en recibir tus datos personales en un formato estructurado, de uso común, de lectura mecánica e interoperable, y puedas transmitirlos a otro responsable del tratamiento, siempre que el tratamiento se legitime en base al consentimiento o en el marco de la ejecución de un contrato. Siempre que sea técnicamente posible, se le transmitirán directamente al responsable del tratamiento destino (por email).
Comentarios	Ver CU-020, aplicado al derecho de portabilidad.

CU-025 – Solicitar Derecho Limitación

Descripción del caso de uso	El solicitante ejerce el derecho de limitación en un sistema de información. Deberá motivar la solicitud por uno de los siguientes supuestos: - Que el tratamiento es ilícito y me opongo a su supresión. - Que el responsable ya no necesita mis datos personales para los fines para los cuales fueron recabados, pero los necesito para la formulación, ejercicio o defensa de mis reclamaciones.
Comentarios	Ver CU-020, aplicado al derecho de limitación.

CU-026 – Solicitar Derecho No decisiones individuales automatizadas.

Descripción del caso de uso	El solicitante ejerce el derecho a no ser objeto de decisiones individuales automatizadas en un sistema de información.
Comentarios	Ver CU-020, aplicado al derecho a no ser objeto de decisiones individuales automatizadas.

CU-027 – Consultar Mis solicitudes

Descripción del caso de uso	El solicitante podrá consultar un listado de las solicitudes presentadas. Y consultar su estado y resolución en caso de estar resueltas.
Actor(es) participante(s)	Solicitante
Secuencia normal	1. El solicitante selecciona la opción de menú “Mis Solicitudes”. 2. El sistema muestra en pantalla un listado con la información relativa a las solicitudes presentadas. Listado: - Este listado contiene las siguientes columnas: o Nombre del Sistema o Derecho ejercido o Estado de la solicitud (Pendiente, En trámite

	o Resuelta). En caso de estar en estado resuelta, aparecerá un botón "Resolución" para acceder a la resolución.
Flujo alternativo 1	2b. Si no existen resultados, se muestra el listado vacío con un mensaje informativo.
Precondición	El solicitante se ha logado en el sistema.
Postcondición	
Comentarios	Figura 60

CU-028 – Consultar Resolución de solicitud presentada

Descripción del caso de uso	El solicitante podrá consultar la resolución de una solicitud resuelta.
Actor(es) participante(s)	Solicitante
Secuencia normal	1. El solicitante pulsa el botón "Resolución" de una solicitud del listado "Mis solicitudes". 2. El sistema muestra una página 2 secciones: - SISTEMA Y SOLICITUD: o Título: el nombre del sistema al que se presenta solicitud. o Responsable del sistema: Nombre e email. o Datos de la solicitud dependientes del derecho ejercido. - RESOLUCION: o Positiva/Negativa. o Observaciones. Descripción justificativa de la resolución adoptada. o En caso de ser una solicitud de Acceso/Portabilidad: ▪ Botón para descargar fichero con datos personales en caso de resolución positiva. o Botón "Volver"
Precondición	El solicitante ha pulsado el botón "Resolución" en una solicitud resuelta del listado "Mis solicitudes".
Postcondición	
Comentarios	Figura 61

CU-029 – Autenticación con Certificado Personal

Descripción del caso de uso	El usuario se autenticará en el sistema con su certificado personal. Si el usuario no está registrado quedará registrado con perfil "Solicitante" en el sistema.
Actor(es) participante(s)	Todos
Secuencia normal	1. El usuario selecciona la opción de menú "Login

	Certificado".
Precondición	El usuario dispone de certificado personal.
Postcondición	Se muestra la home del usuario según perfil.
Comentarios	Figuras del Modelo de Pantallas

CU-030 – Autenticación con usuario/password.

Descripción del caso de uso	El usuario se autenticará en el sistema con su usuario/password.
Actor(es) participante(s)	Todos
Secuencia normal	1. El usuario selecciona la opción de menú "Login (user/pwd)". 2. El sistema muestra en pantalla un formulario para autenticarse con usuario y password. 3. El usuario introduce su usuario/password y pulsa "Acceder"
Flujo alternativo 1	3b. Usuario/password incorrectos.
Precondición	El usuario está registrado en el sistema.
Postcondición	Se muestra la home del usuario según perfil.
Comentarios	Figura 47

CU-031 – Logout

Descripción del caso de uso	El usuario abandona el sistema.
Actor(es) participante(s)	Todos
Secuencia normal	1. El administrador pulsa el botón de la cabecera "Logout". 2. El sistema muestra la página "home" con las opciones de login.
Precondición	El usuario se ha autenticado en el sistema.
Postcondición	Usuario no autenticado
Comentarios	Figura 46

CU-032 – Firmar

Descripción del caso de uso	El solicitante firma una solicitud.
Actor(es) participante(s)	Solicitante
Secuencia normal	1. El Solicitante pulsa el botón "Firmar y enviar". 2. El sistema lanza la aplicación "Autofirma". 3. El usuario selecciona su certificado personal y pulsa "Aceptar"
Precondición	El usuario se ha autenticado en el sistema. El usuario tiene instalado "Autofirma" en su equipo.

Postcondición	
Comentarios	

CU-033 – Cambiar Idioma

Descripción del caso de uso	El usuario podrá seleccionar cambiar de idioma entre los configurados en el sistema.
Actor(es) participante(s)	Todos
Secuencia normal	1. El usuario pulsa el botón de idioma seleccionado.
Precondición	El usuario accede a la home.
Postcondición	La web cambia al idioma seleccionado.
Comentarios	

2.4 Modelo de clases de Análisis

Basándonos en la especificación de requisitos y de casos de uso previo, paso a identificar las clases del modelo del dominio de nuestro sistema, sus atributos y las relaciones entre ellas.

2.4.1 Diagrama de clases

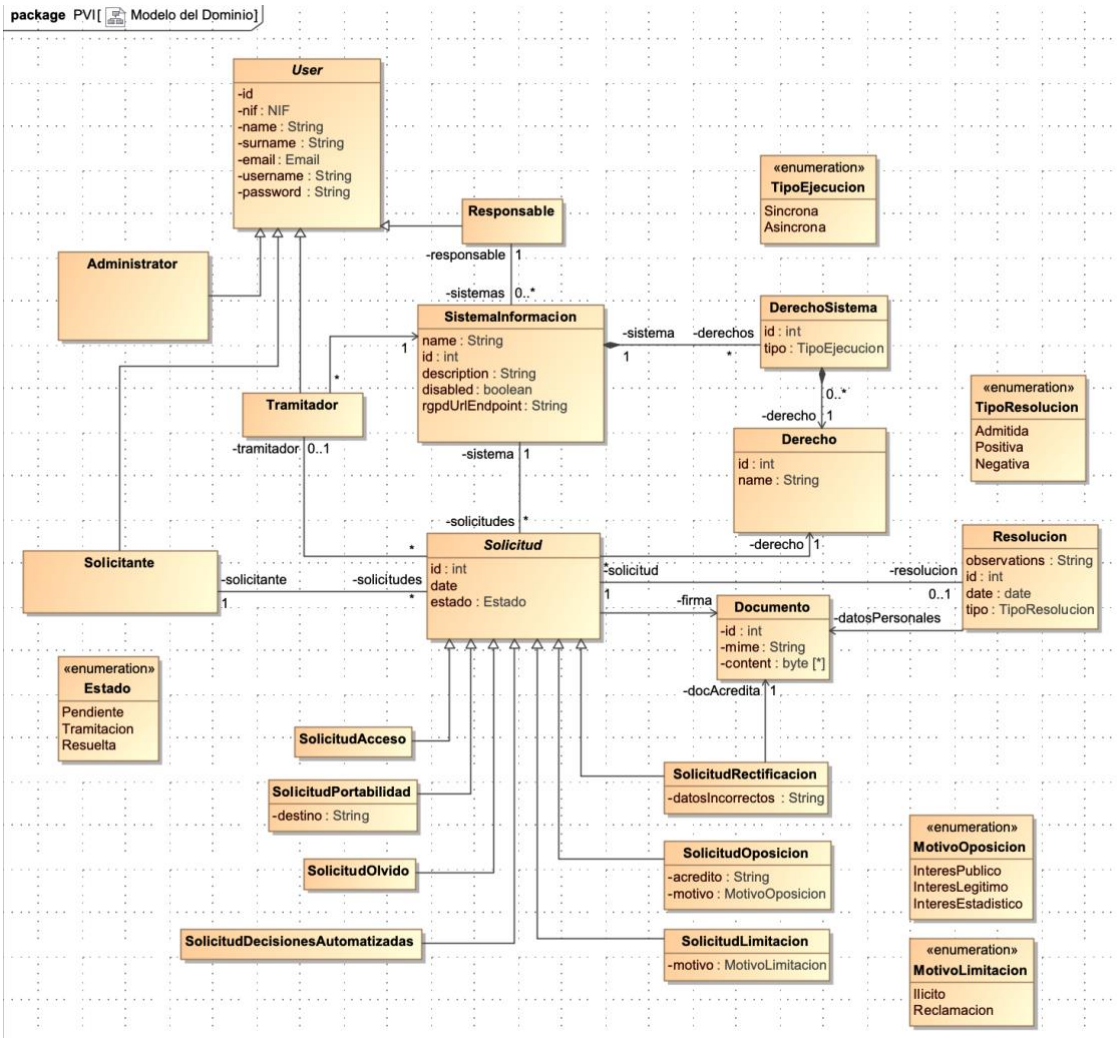


Figura 9. Diagrama de Clases

2.4.2 Semántica de las clases

Pasamos a describir las clases del dominio, sus relaciones y sus atributos más importantes.

User

Clase base de todos los usuarios del sistema eRGPD.
Atributos:

- Id. SerialNumber del Certificado Personal del usuario.
- Nif.
- Name. Nombre del usuario
- Surname. Apellidos
- Username. Nombre de usuario para login user/pwd
- Password. Contraseña para login user/pwd
- Email. Correo electrónico para notificaciones.

Solicitante

Clase de usuario que representa a un interesado que ejerce un derecho contemplado en el RGPD en uno de los sistemas de información gestionados. Se registrará en el sistema la primera vez que acceda con su certificado personal. Cada vez que ejerce un derecho se registra una solicitud.
Relaciones:

- Solicitud. Solicitudes presentadas.

Tramitador

Clase de usuario que representa a un tramitador de solicitudes (asíncronas) de un sistema de información gestionado por eRGPD.
Relaciones:

- SistemaInformacion: Sistema del cual es tramitador.
- Solicitud. Solicitudes que está tramitando o ha resuelto.

Responsable

Clase de usuario que representa al responsable de un sistema de información (figura responsable del tratamiento del RGPD).
Relaciones:

- Sistema de información. Un responsable puedes serlo de varios sistemas de información.

Administrador

Clase de usuario con permisos para gestionar los sistemas de información, dar de alta al resto de usuarios de la organización (administradores, tramitadores y responsables). Es el encargado de configurar los sistemas de información.

Derecho

Clase de representa un derecho de los interesados recogidos en el RGPD, Se inicializan en el sistema eRGPD en la carga inicial de datos.
Atributos:

- Id. identificador
- name. Nombre del derecho RGPD.

Relaciones:

- Solicitud. Solicitudes presentadas.
- DerechoSistema. Sistemas y su tipo de ejecución.

DerechoSistema

Clase de representa la relación entre los sistemas de información de la organización que tratan datos personales gestionados y los derechos del RGPD. Al dar de alta un sistema, se crean instancias del sistema con todos los derechos en modo asíncrono.
Atributos:

- TipoEjecución.

Relaciones:

- SistemaInformacion.
- Derecho.

TipoEjecucion

Enumerado que representa los modos de tramitar la solicitud:

- Sincrona. Tramitación instantánea a través de web service
- Asincrona. Tramitación atendida por usuario tramitador.

Solicitud

Clase base que representa una petición del Solicitante al ejercer un derecho sobre un sistema de información gestionado por eRGPD.
Atributos:

- Id. Identificador
- Date. Timestamp del momento de solicitar.

Relaciones:

- Solicitante. Usuario que realiza la petición.
- SistemaInformacion. Sistema gestionado al que se le presenta la solicitud.
- Derecho. Derecho de la solicitud presentada.
- Tramitador. En caso de ser procesado de manera asíncrona, registrará el tramitador que la gestione.
- Documento. Firma electrónica de la solicitud.
- Estado. Estado de la solicitud.
- Resolución. Resolución de la petición una vez tramitada.

Estado

Enumerado que representa los distintos estados por los que puede pasar una solicitud:

- Pendiente. No tramitada.
- Tramitación. En proceso de tramitación por un tramitador.
- Resuelta. Atendida y con resolución.

SolicitudAcceso

Clase de solicitud del derecho de acceso.

SolicitudRectificación

Clase de solicitud del derecho de rectificación.
Atributos:

- datosIncorrectos. Que datos se solicitan rectificar.

Relaciones:

- Documento. Documentación que acredita la rectificación.

SolicitudOlvido

Clase de solicitud del derecho de supresión (al olvido).

SolicitudPortabilidad

Clase de solicitud del derecho a la portabilidad.
Atributos:

- Destino. Email destinatario de los datos personales a portar.

SolicitudOposición

Clase de solicitud del derecho de oposición.
Atributos:

- Acredito. Situación personal que acredita ejercer el derecho.

Relaciones:

- MotivoOposición. Motivo.

MotivoOposicion

Enumerado que representa los motivos a tener en cuenta:

- InteresPublico.
- InteresLegitimo.
- InteresEstadistico.

SolicitudLimitacion

Clase de solicitud del derecho a la limitación del tratamiento.
Relaciones:

- MotivoOposición. Motivo.

MotivoLimitacion

Enumerado que representa los motivos a considerar:

- Ilicito.
- Reclamacion.

SolicitudDecisionesAutomatizadas

Clase de solicitud del derecho a no ser objeto de decisiones individuales automatizadas.

SistemaInformacion

Clase que representa un sistema de información que trate datos personales en la organización.
Atributos:

- Id. identificador
- Nombre. Nombre del sistema de información
- Description. Descripción del sistema
- Disabled. Si está deshabilitado. Solo se pueden presentar solicitudes en sistemas habilitados.
- rgpdUrlEndpoint. Url del endpoint que implementa el web service que trata las peticiones síncronas del sistema de información.

Relaciones:

- Responsable. Usuario responsable del tratamiento.
- Tramitador. Usuarios tramitadores.
- Solicitud. Solicitudes presentadas.
- DerechoSistema. Derechos y su tipo de ejecución.

Resolucion

Clase de representa la resolución a la solicitud en tramitación o tramitada.
Atributos:

- Id. identificador
- observations. Justificación de la resolución.
- Date. Timestamp del momento de resolver.

Relaciones:

- Solicitud.
- Documento. En caso de solicitud de acceso o portabilidad, documento con los datos personales del solicitante que trata el sistema de información.
- TipoResolucion.

TipoResolucion

Enumerado que representa el estado de la resolución:

- Admitida. Tramitándose por un tramitador.
- Positiva. Resuelta favorable al solicitante
- Negativa. Resuelta desfavorable al solicitante.

3. Diseño

3.1 Arquitectura del sistema

La arquitectura elegida para diseñar el sistema es una arquitectura heterogénea basada en:

- Cliente-servidor: organizado en capas horizontales definidas por el grado de cercanía al usuario. La distribución por capas favorece la escalabilidad y permite aislar las funcionalidades que proporcionan con interfaces muy definidas.
- Orientada a objetos distribuidos: Diseño los elementos de cada capa como objetos distribuidos, proporcionando escalabilidad al sistema.

3.2 Diagrama de Arquitectura

En un primer diagrama de componentes describo la arquitectura de 3 capas representadas en paquetes, los distintos componentes y las interfaces que publican para comunicarse con las capas superiores.
Por motivos de legibilidad, el diagrama general mostrará las interfaces colapsadas, y posteriormente, pasaré a expandir los interfaces de los distintos componentes para mostrar la firma de los servicios que ofrecen en detalle.

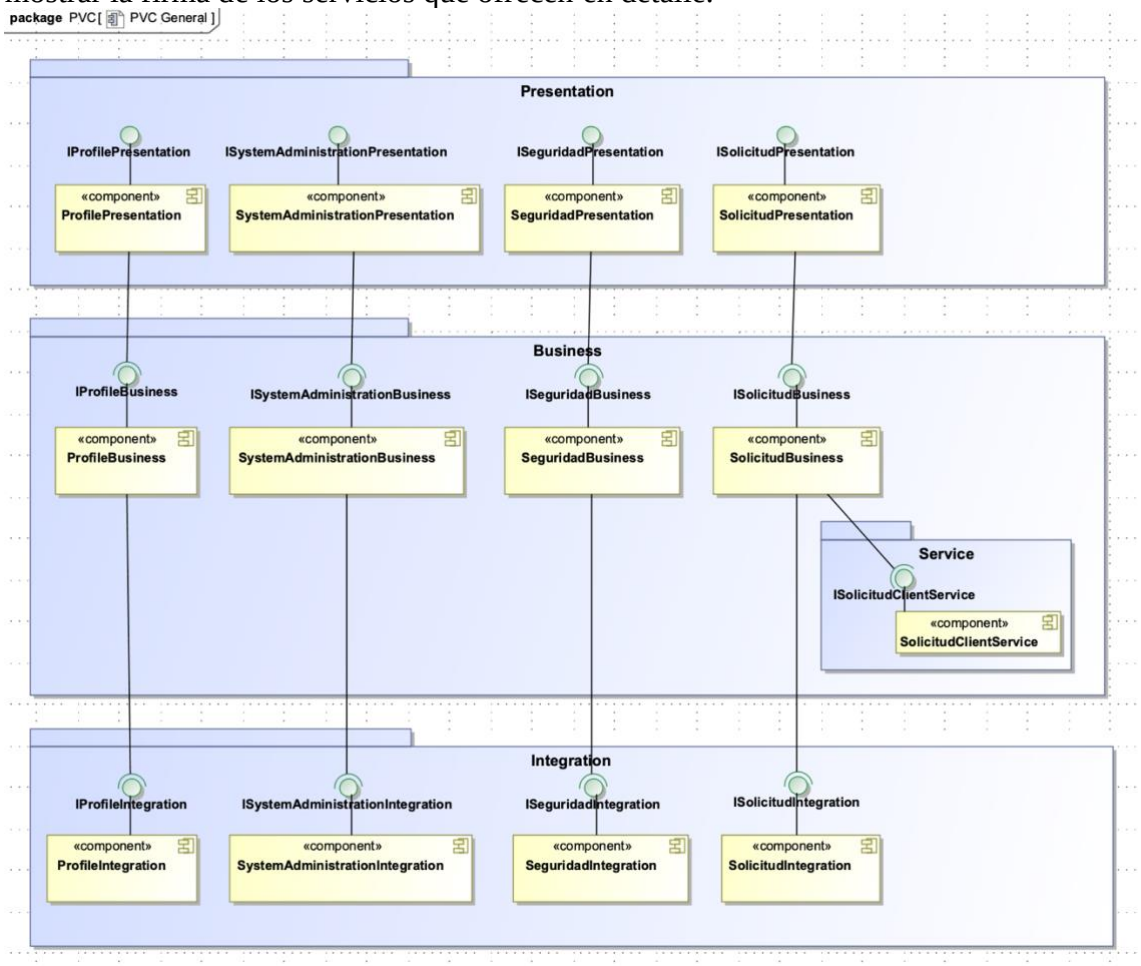


Figura 10. Diagrama de Arquitectura

Como se puede observar en el diagrama de arquitectura anterior, he definido 4 componentes principales (en cada capa, presentación, negocio y persistencia) que se corresponden con la organización funcional que especificamos en el diagrama de casos de uso:

- Seguridad
- Profile
- Solicitudes
- SystemAdministration

Además, definimos un componente en la capa de negocio, "SolicitudService", encargado de la tramitación de las solicitudes de manera síncrona, responsable de la comunicación con los sistemas de información de la organización gestionados por eRGPD que usan datos personales.

3.2.1 Presentación

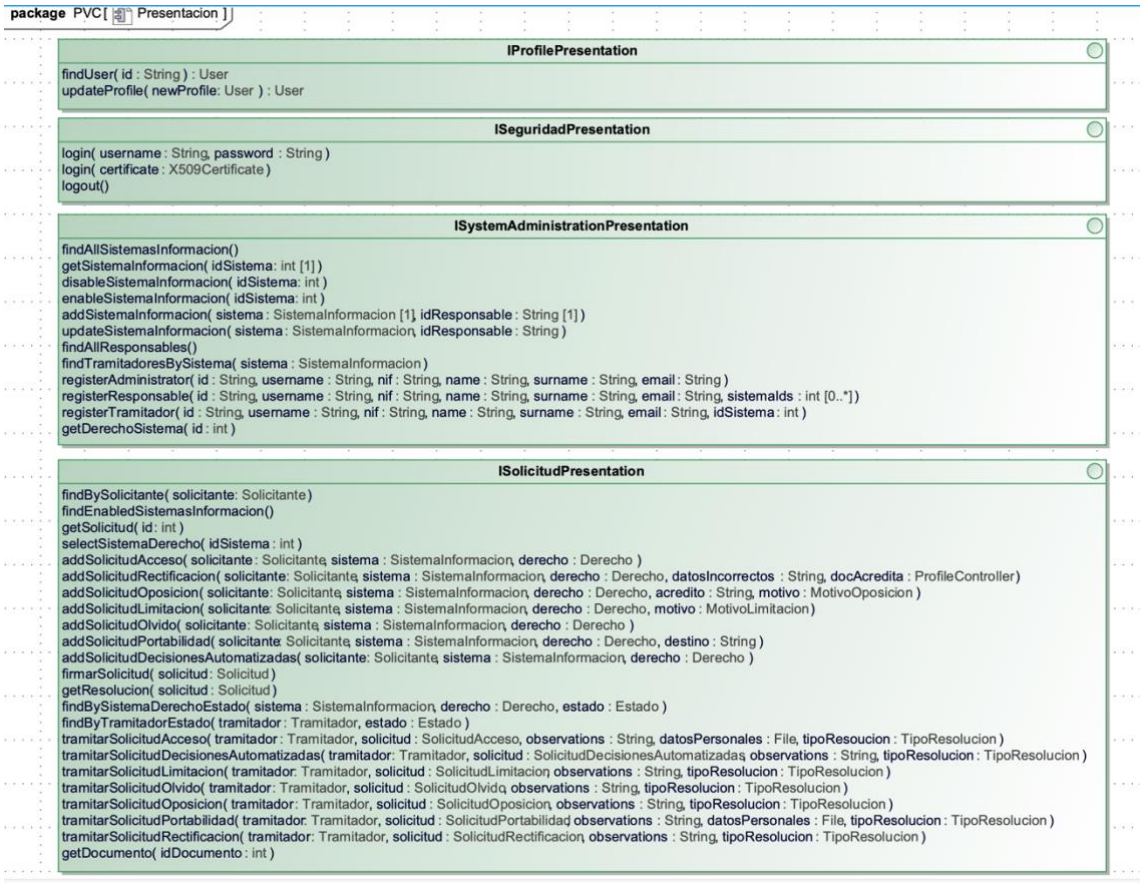


Figura 11. Interfaces Capa Presentación

3.2.2 Business

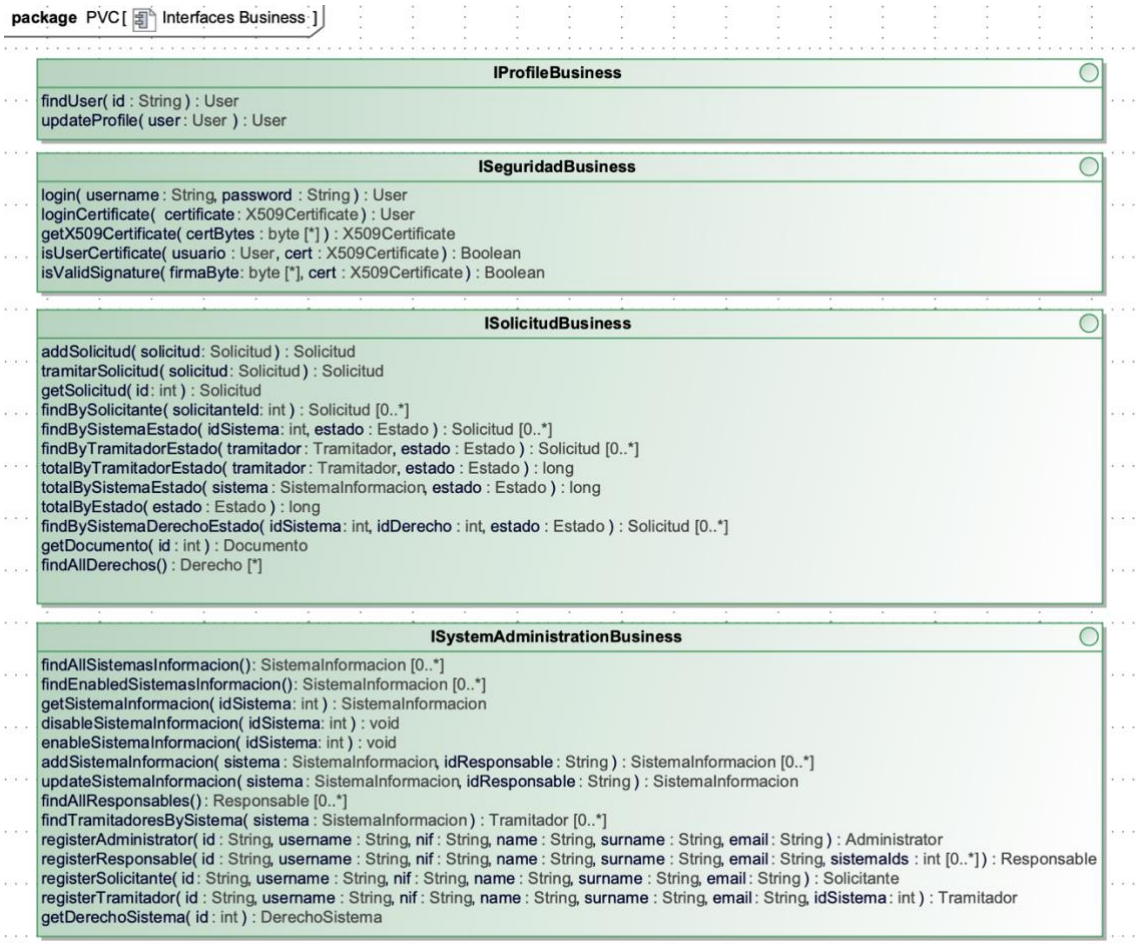


Figura 12. Interfaces Capa Negocio

3.2.2.1 Cliente Servicio tramitación síncrona:

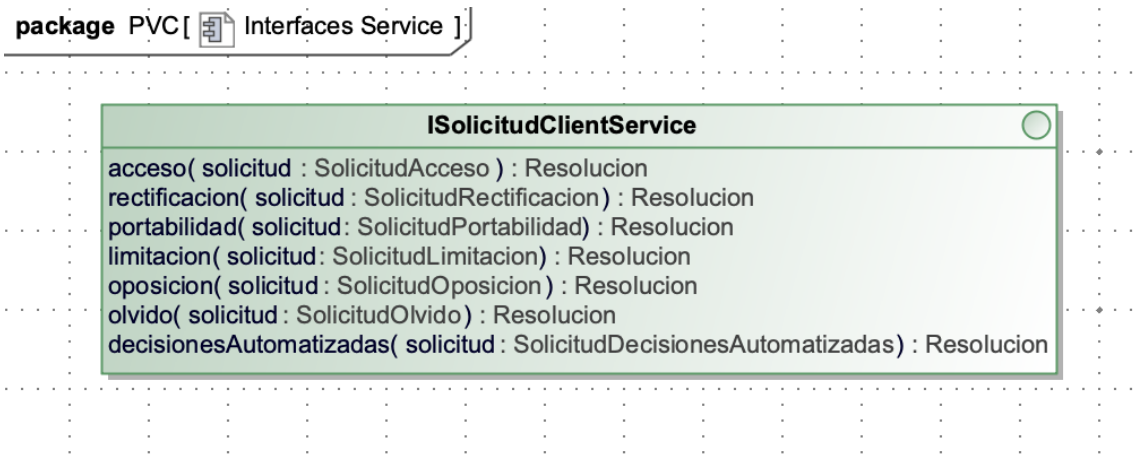


Figura 13. Interface Service Tramitación Síncrona

3.2.3 Integration

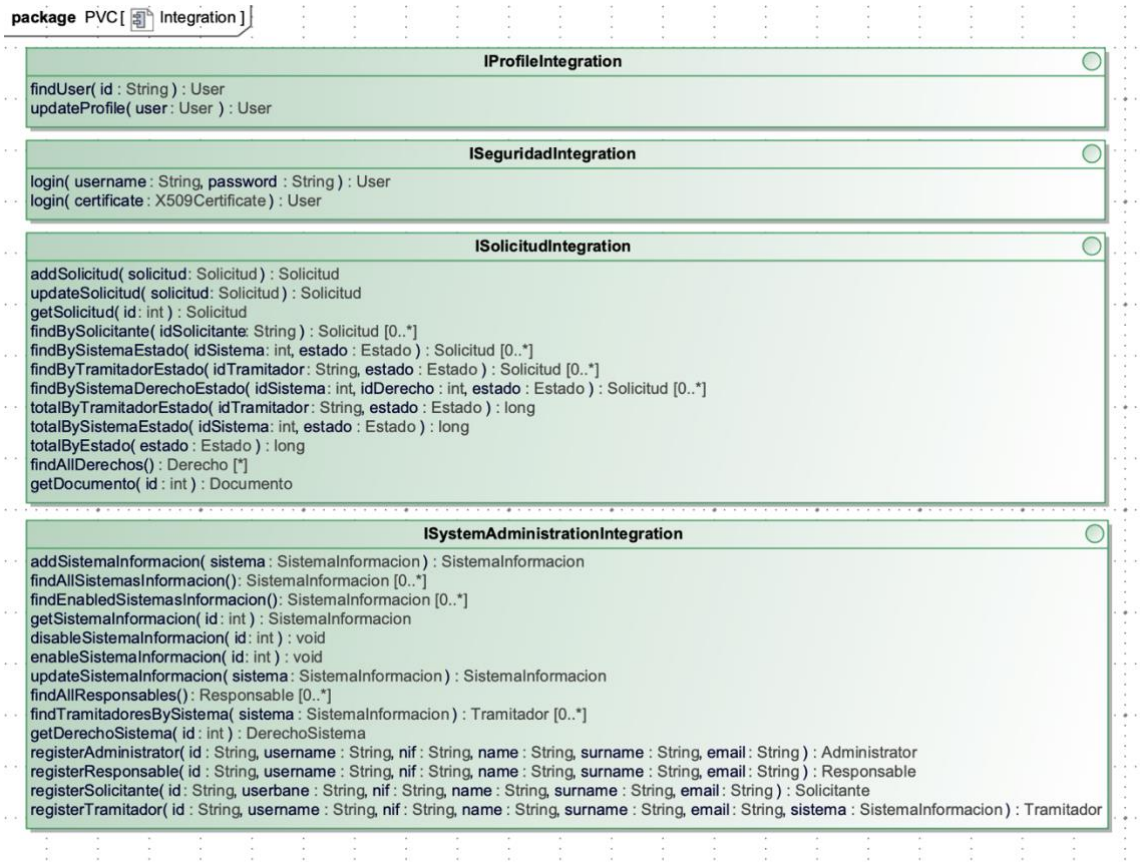


Figura 14. Interfaces Capa Persistencia

3.3 Refinamientos

3.3.1 Presentación

Paso a refinar la capa de presentación siguiendo el patrón de diseño Modelo-Vista-Controlador, dado que el modelo estará implementado en la capa de negocio, en un **primer refinamiento** dividiré los distintos componentes de presentación en 2 componentes: controlador y vista.

A continuación, se llevará a cabo un **segundo refinamiento** basado en la aplicación de los siguientes patrones de diseño:

- FrontController: controlador para centralizar en un único punto las peticiones del usuario, delegando en otros componentes la generación de la vista adecuada a la petición.
- Command. Encapsulación de las acciones del usuario, teniendo por cada acción una vista asociada, pudiendo reutilizarlas cuando sea posible.

Por último, aplicaré el **perfil J2EE**, teniendo en cuenta que usaré Java Server Faces (JSF) para esta capa, tecnología perteneciente a la especificación J2EE que cumple con el patrón MVC seleccionado previamente, tendremos la siguiente relación:

- FrontController: FacesServlet.
- Actions: ManagedBeans
- Views: facelets.

ProflePresentation

Primer Refinamiento

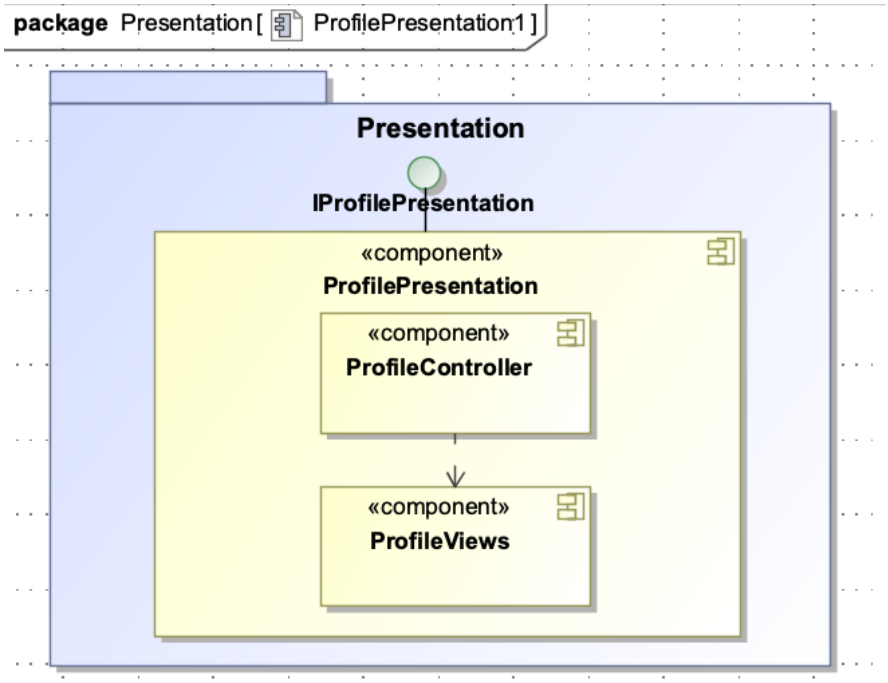


Figura 15. ProfilePresentation. Primer refinamiento

Segundo Refinamiento

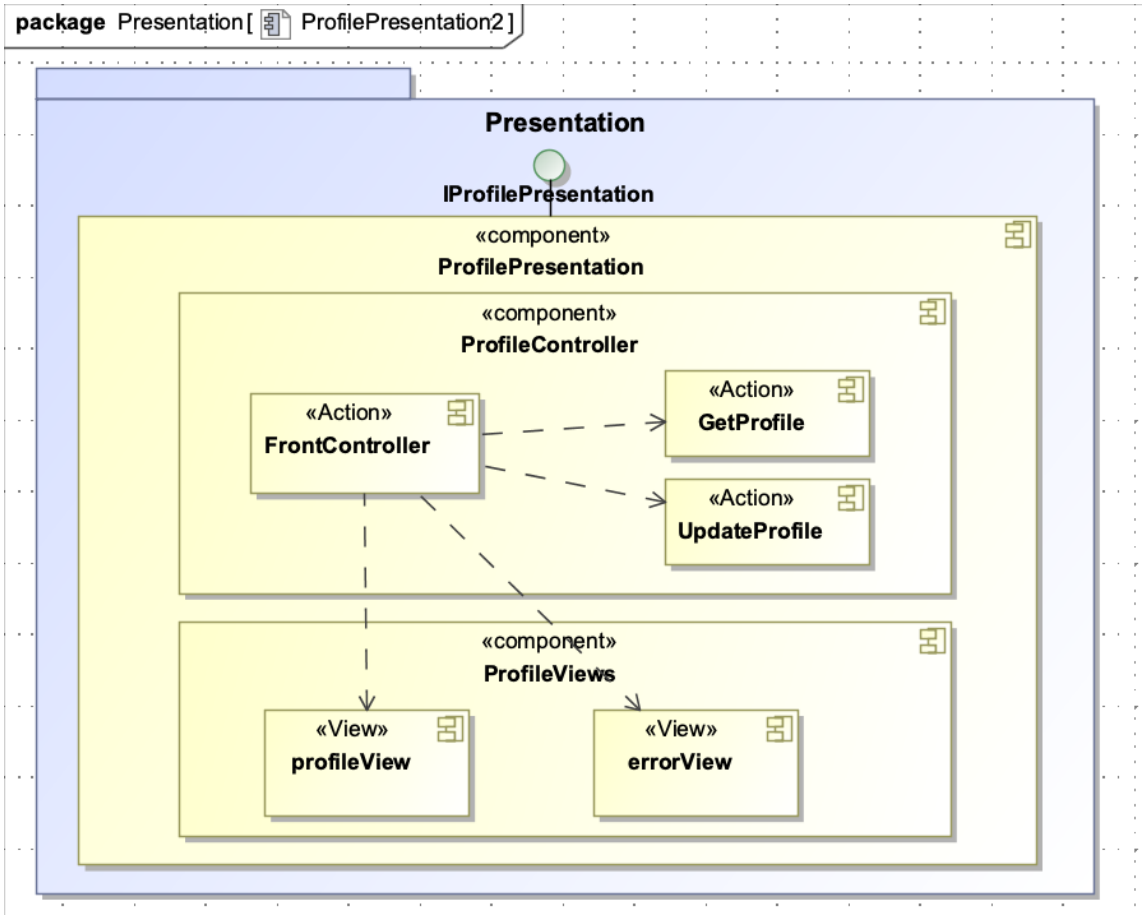


Figura 16. ProfilePresentation. Segundo refinamiento

Como resultado de este segundo refinamiento, obtenemos las siguientes acciones y vistas:

- Acciones:
  - GetProfile: Obtiene el perfil del usuario logado
  - UpdateProfile: Actualiza el perfil del usuario
- Vistas:
  - profileView. Formulario con los datos del perfil del usuario.
  - errorView. Vista genérica para visualizar errores.

Perfil J2EE

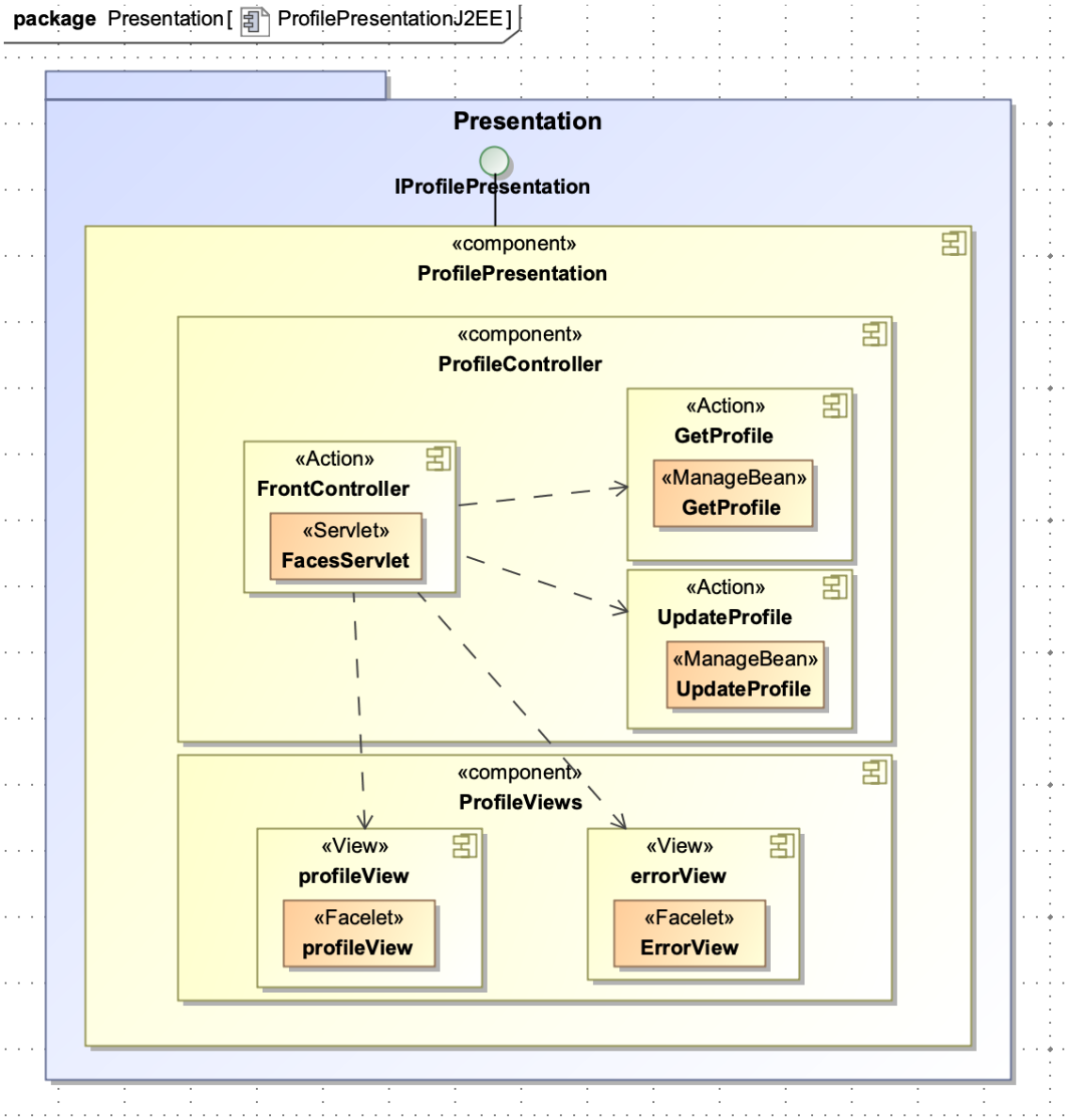


Figura 17. ProfilePresentation. Perfil J2EE

SeguridadPresentation

Primer Refinamiento

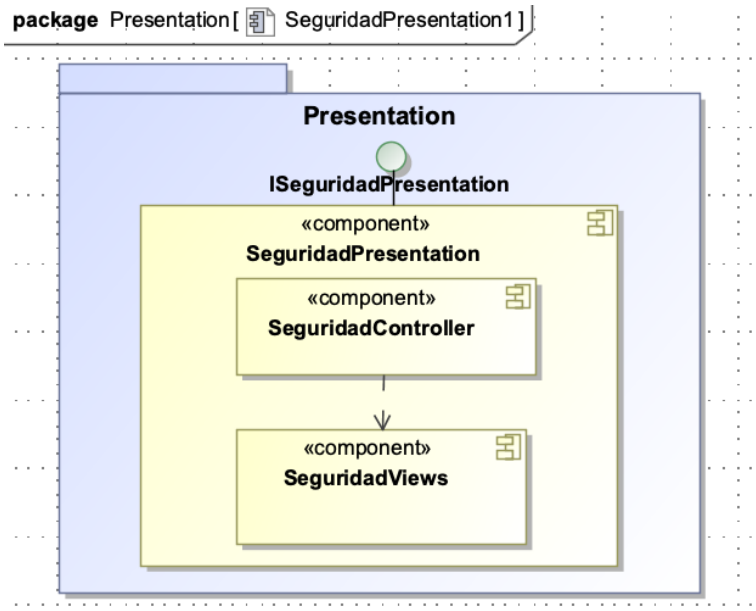


Figura 18. SeguridadPresentation. Primer refinamiento

Segundo Refinamiento

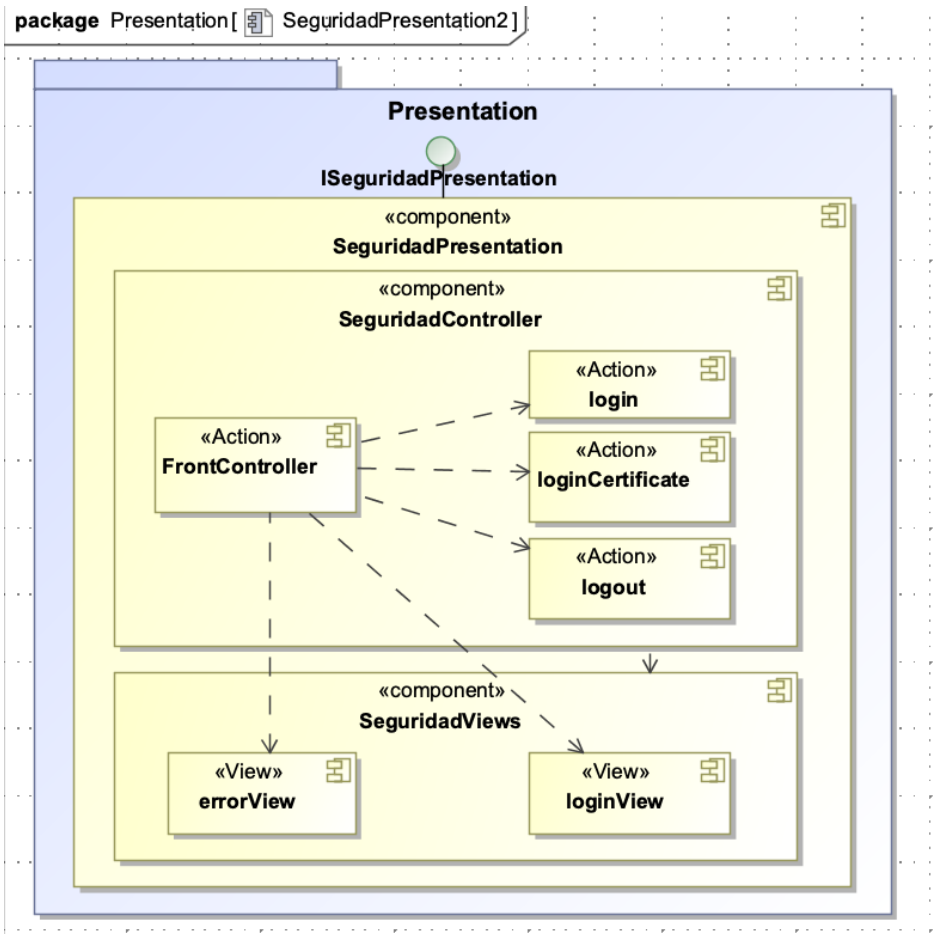


Figura 19. SeguridadPresentation. Segundo refinamiento

Como resultado de este segundo refinamiento, obtenemos las siguientes acciones y vistas:

- Acciones:
  - login: logarse con usuario y password.
  - loginCertificate: login con certificado personal
  - logout
- Vistas:
  - loginView. Formulario login con usuario y password.
  - errorView. Vista genérica para visualizar errores.

Perfil J2EE

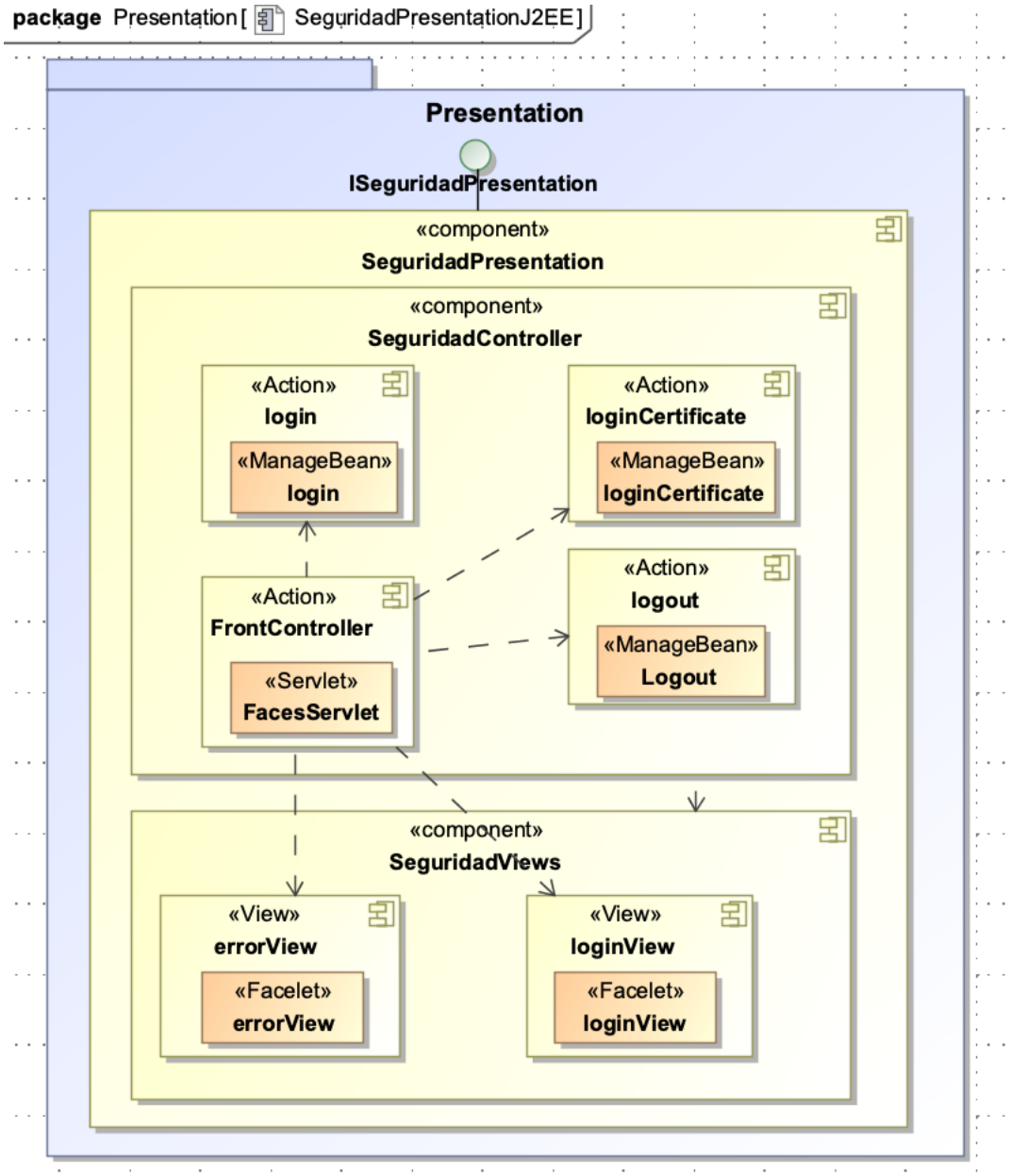


Figura 20. SeguridadPresentation. Perfil J2EE

SystemAdministrationPresentation

Primer Refinamiento

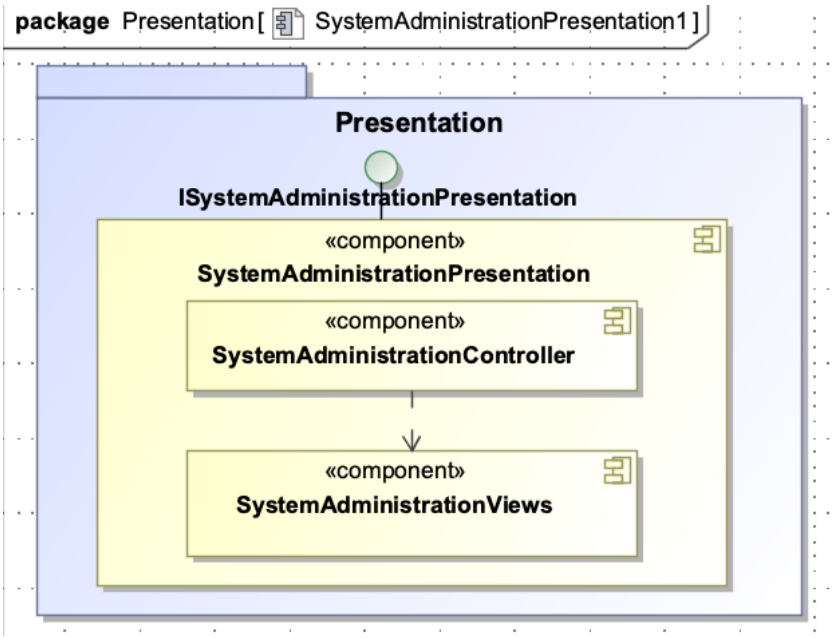


Figura 21. SystemAdministrationPresentation. Primer refinamiento

Segundo Refinamiento

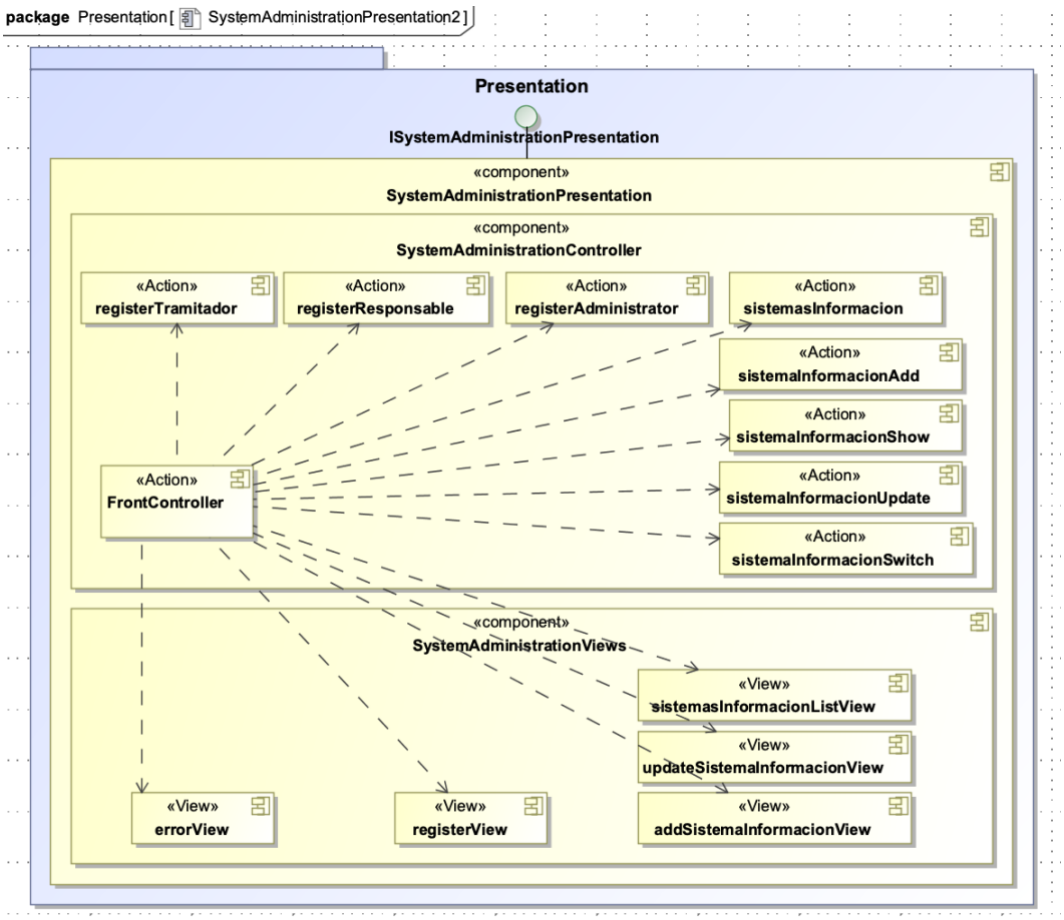


Figura 22. SystemAdministrationPresentation. Segundo refinamiento

Como resultado de este segundo refinamiento, obtenemos las siguientes acciones y vistas:

- Acciones:
  - registerTramitador: da de alta a un tramitador en un sistema.
  - registerAdministrador: da de alta un administrador
  - registerResponsable: da de alta un responsable del tratamiento.
  - sistemasInformacion: lista todos los sistemas de información gestionados.
  - sistemaInformacionAdd: da de alta un nuevo sistema de información.
  - sistemaInformcionUpdate: actualiza un sistema de información. Asignándole tipos de ejecución síncrona o asíncrona a cada uno de los derechos del interesado.
  - sistemaInformacionSwitch: Habilita/Deshabilita un sistema de informción.
- Vistas:
  - sistemasInformcionListView. Listado de los sistemas de información gestionados.
  - addSistemaInformacionView: formulario de alta de un nuevo sistema.
  - updateSistemaInformacionView: formulario edición de la configuración del sistema.
  - errorView. Vista genérica para visualizar errores.

Perfil J2EE

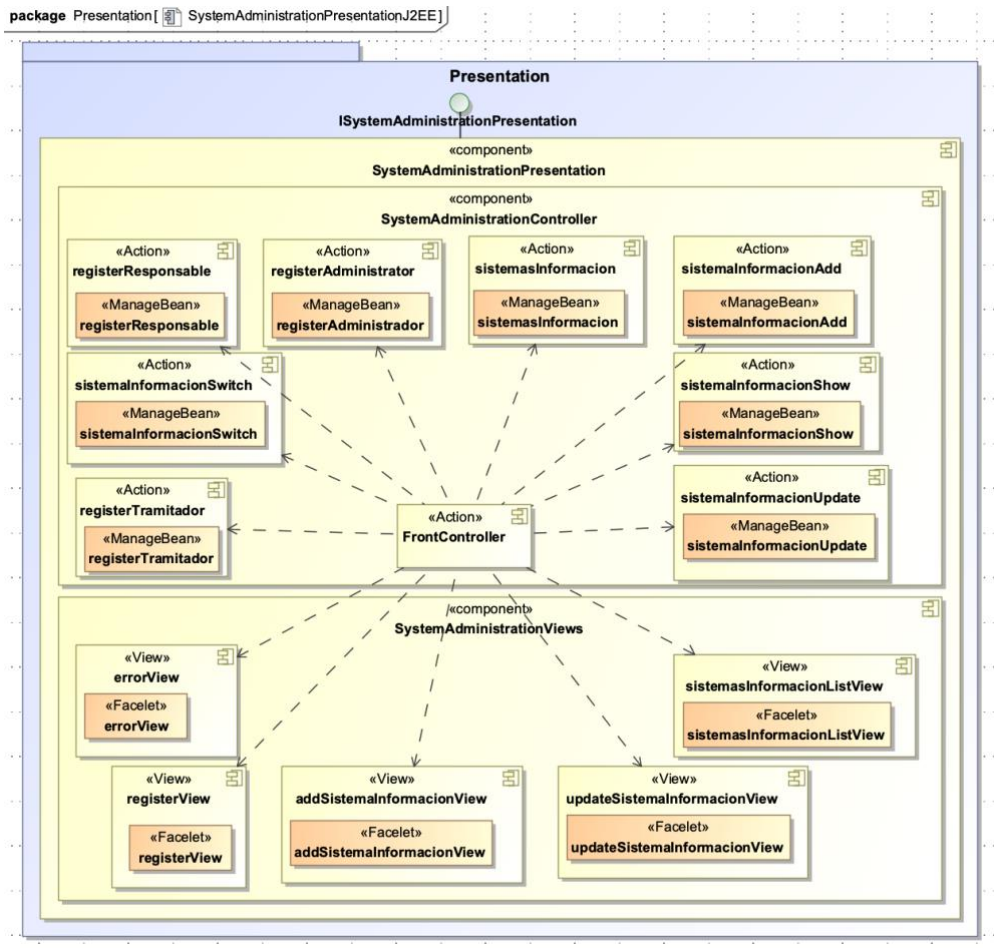


Figura 23. SystemAdministrationPresentation. Perfil J2EE

SolicitudesPresentation

Primer Refinamiento

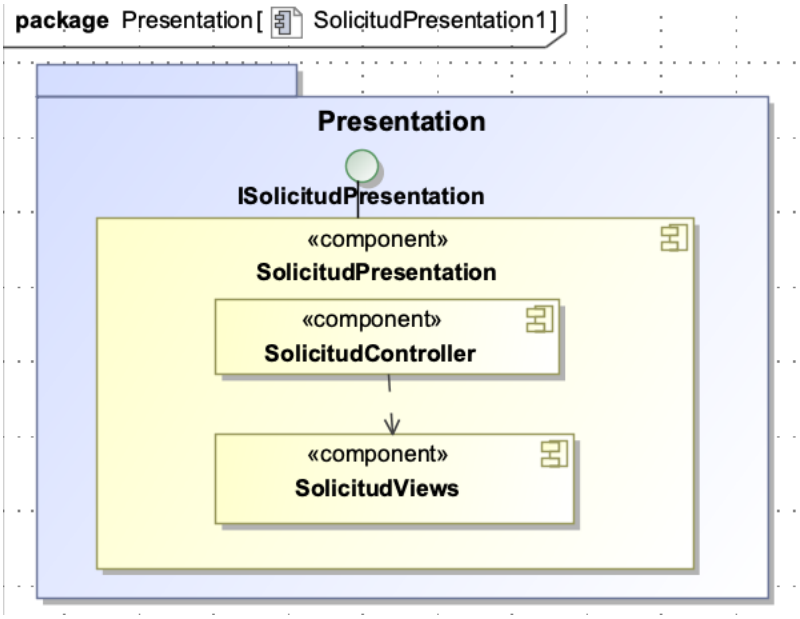


Figura 24. SolicitudPresentation. Primer refinamiento

Segundo Refinamiento

Voy a organizar el componente de Solicitudes (principal entidad del sistema) por su complejidad en 3 paquetes definidos por los actores implicados.
Así, tendremos:

Solicitante

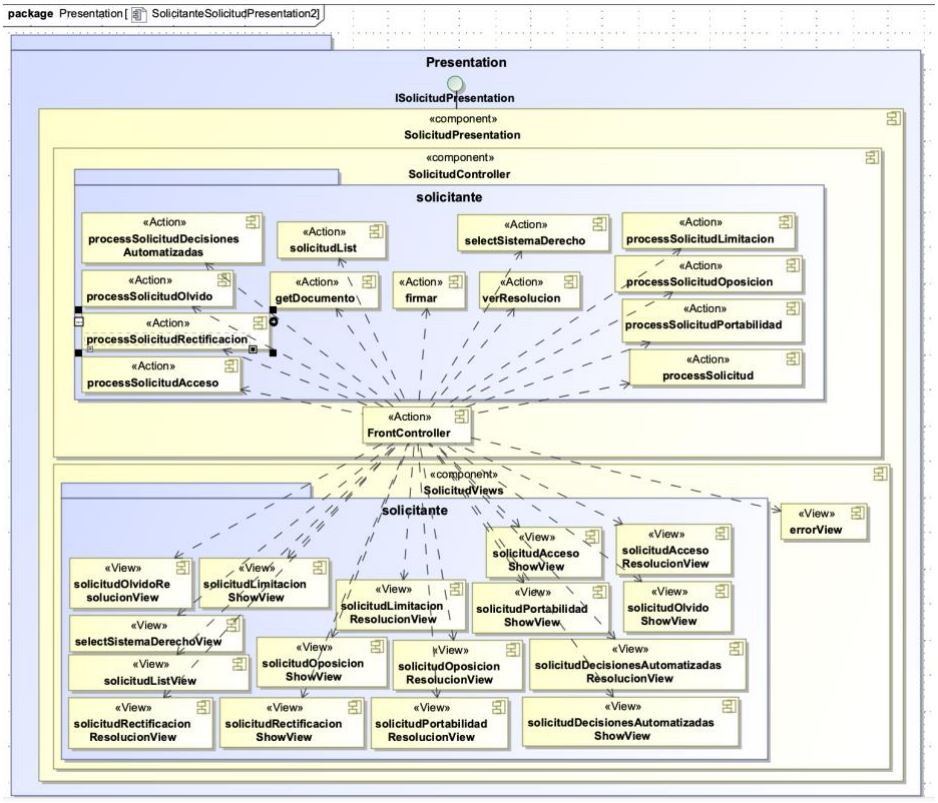


Figura 25. SolicitudPresentation. Solicitante Segundo refinamiento

Como resultado de este segundo refinamiento, para el solicitante obtenemos las siguientes acciones y vistas:

- Acciones:
    - solicitudList: Solicitudes presentadas por el solicitante.
    - selectSistemaDerecho: selección del sistema y derecho al que se va a presentar la solicitud.
    - processSolicitud: solicitar el derecho seleccionado.
    - processSolicitudAcceso. Presentar la solicitud de acceso.
    - processSolicitudDecisionesAutomatizadas. Presentar la solicitud a no ser objeto de decisiones individuales automatizadas.
    - processSolicitudRectificacoion. Presentar la solicitud de rectificación.
    - processSolicitudLimitacion. Presentar la solicitud a la limitación del tratamiento.
    - processSolicitudOposicion. Presentar la solicitud de oposición.
    - processSolicitudPortabilidad. Presentar la solicitud a la portabilidad.
    - processSolicitudOlvido. Presentar la solicitud de supresión (al olvido).
    - getDocumento. Descarga documentos de datos personales de las resoluciones favorables al interesado en los derechos de acceso y portabilidad.
    - verResolucion. Ver la resolución de una solicitud resuelta.
    - Firmar. Firmar la solicitud con el certificado personal a través de la aplicación Autofirma.
- Vistas:
    - solicitudListView. Listado de mis solicitudes.
    - selectSistemaDerechoView. Formulario con dos combos de selección, sistema y derecho. Dependiendo de la selección hecha, se actualizará una nota informativa con el modelo de respuesta del sistema para esa combinación (síncrona o asíncrona).
    - solicitudAccesoShowView. Formulario con información de la solicitud de acceso.
    - solicitudAccesoResolucionView. Resolución de la solicitud de acceso seleccionada y acceso a descargar los datos personales si la resolución es favorable al interesado.
    - solicitudRectificacionShowView. Formulario con información de la solicitud de rectificación y los datos a cumplimentar, datos incorrectos y documentación que lo acredita.
    - solicitudRectificacionResolucionView. Resolución de la solicitud de rectificación seleccionada.
    - solicitudLimitacionShowView. Formulario con información de la solicitud de limitación y los datos a cumplimentar, motivo a considerar.
    - solicitudLimitacionResolucionView. Resolución de la solicitud de limitación seleccionada.
    - solicitudOposicionShowView. Formulario con información de la solicitud de oposición y los datos a cumplimentar, motivo y situación personal que acredita.
    - solicitudOposicionResolucionView. Resolución de la solicitud de oposición seleccionada.

- solicitudPortabilidadShowView. Formulario con información de la solicitud de portabilidad y los datos a cumplimentar, el destino de los datos personales del solicitante.
- solicitudPortabilidadResolucionView. Resolución de la solicitud de portabilidad seleccionada, con posibilidad de descarga de los datos personales del interesado.
- solicitudOlvidoShowView. Formulario con información de la solicitud de supresión (al olvido).
- solicitudAccesoResolucionView. Resolución de la solicitud de supresión seleccionada.
- solicitudDecisionesAutomatizadasShowView. Formulario con información de la solicitud a no ser objeto de decisiones individuales automatizadas.
- solicitudDecisionesAutomatizadasResolucionView. Resolución de la solicitud a no ser objeto de decisiones individuales automatizadas seleccionada.
- errorView. Vista genérica para visualizar errores.

Tramitador

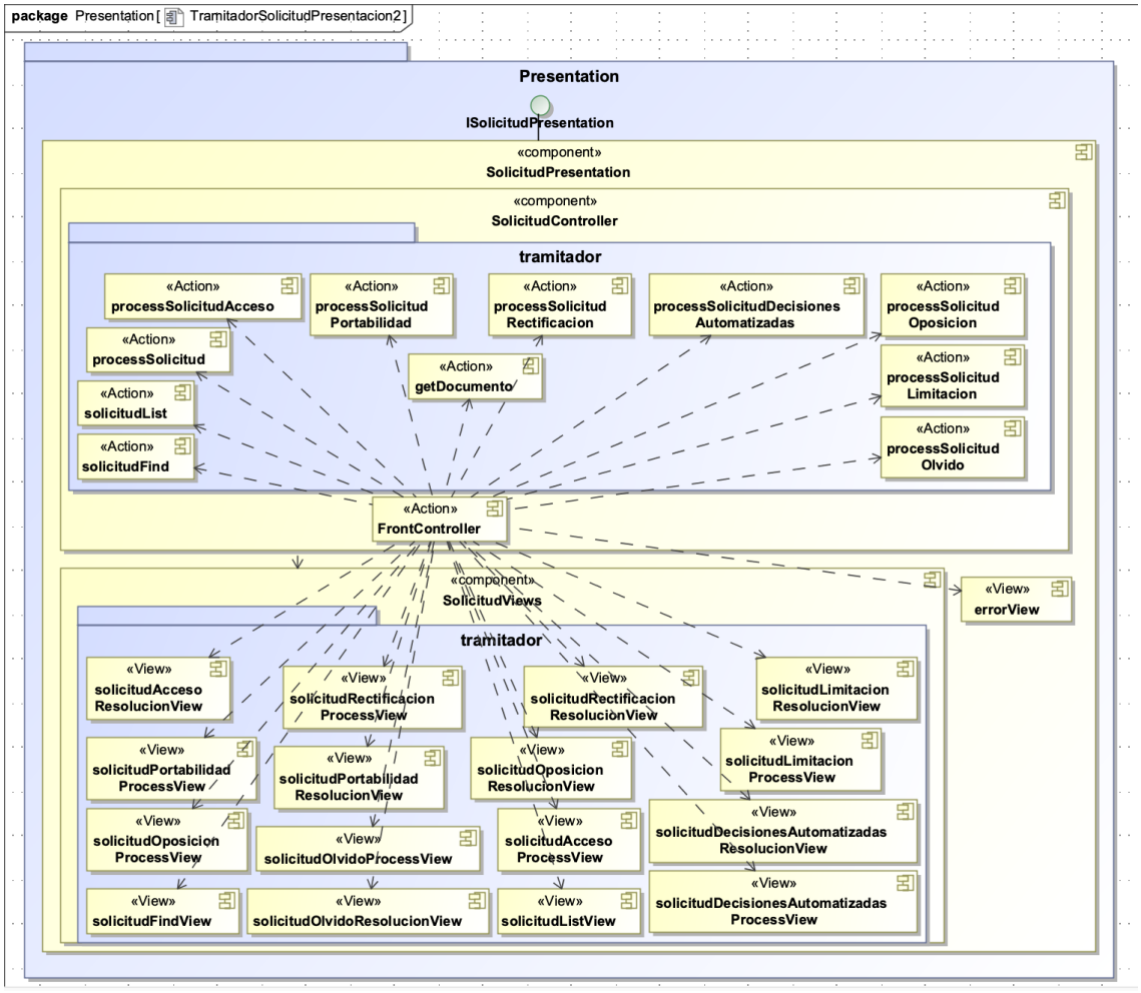


Figura 26. SolicitudPresentation. Tramitador Segundo refinamiento

Como resultado de este segundo refinamiento, para el tramitador obtenemos las siguientes acciones y vistas:

- Acciones:
    - solicitudList: listado de solicitudes pendientes de tramitar en el sistema (sin tramitador procesándolas), en tramitación y resueltas por el tramitador logado.
    - solicitudFind: buscar solicitudes filtrando por derecho y estado de la solicitud.
    - processSolicitudAcceso. Tramitar la solicitud de acceso.
    - processSolicitudDecisionesAutomatizadas. Tramitar la solicitud a no ser objeto de decisiones individuales automatizadas.
    - processSolicitudRectificacoion. Tramitar la solicitud de rectificación.
    - processSolicitudLimitacion. Tramitar la solicitud a la limitación del tratamiento.
    - processSolicitudOposicion. Tramitar la solicitud de oposición.
    - processSolicitudPortabilidad. Tramitar la solicitud a la portabilidad.
    - processSolicitudOlvido. Tramitar la solicitud de supresión (al olvido).
    - getDocumento. Descarga documentos: aportados por el solicitante en la solicitud, y datos personales en la consulta de las resoluciones.
- Vistas:
    - solicitudListView. Listado de solicitudes del sistema.
    - solicitudAccesoProcessView. Formulario con información de la solicitud de acceso presentada y los campos necesarios para resolverla, observaciones y un fichero con los datos personales del interesado.
    - solicitudAccesoResolucionView. Resolución de la solicitud de acceso seleccionada y acceso a descargar los datos personales si la resolución es favorable al interesado.
    - solicitudRectificacionProcessView. Formulario con información de la solicitud de rectificación y los campos necesarios para resolverla, observaciones.
    - solicitudRectificacionResolucionView. Resolución de la solicitud de rectificación seleccionada.
    - solicitudLimitacionProcessView. Formulario con información de la solicitud de limitación y los campos necesarios para resolverla, observaciones.
    - solicitudLimitacionResolucionView. Resolución de la solicitud de limitación seleccionada.
    - solicitudOposicionProcessView. Formulario con información de la solicitud de oposición y los campos necesarios para resolverla, observaciones.
    - solicitudOposicionResolucionView. Resolución de la solicitud de oposición seleccionada.
    - solicitudPortabilidadProcessView. Formulario con información de la solicitud de portabilidad y los campos necesarios para resolverla, observaciones y los datos personales del interesado que se van a portar.
    - solicitudPortabilidadResolucionView. Resolución de la solicitud de portabilidad seleccionada, con posibilidad de descarga de los datos personales del interesado.

- solicitudOlvidoProcessView. Formulario con información de la solicitud de supresión (al olvido) y los campos necesarios para resolverla, observaciones.
- solicitudAccesoResolucionView. Resolución de la solicitud de supresión seleccionada.
- solicitudDecisionesAutomatizadasProcessView. Formulario con información de la solicitud a no ser objeto de decisiones individuales automatizadas y los campos necesarios para resolverla, observaciones.
- solicitudDecisionesAutomatizadasResolucionView. Resolución de la solicitud a no ser objeto de decisiones individuales automatizadas seleccionada.
- errorView. Vista genérica para visualizar errores.

Responsable

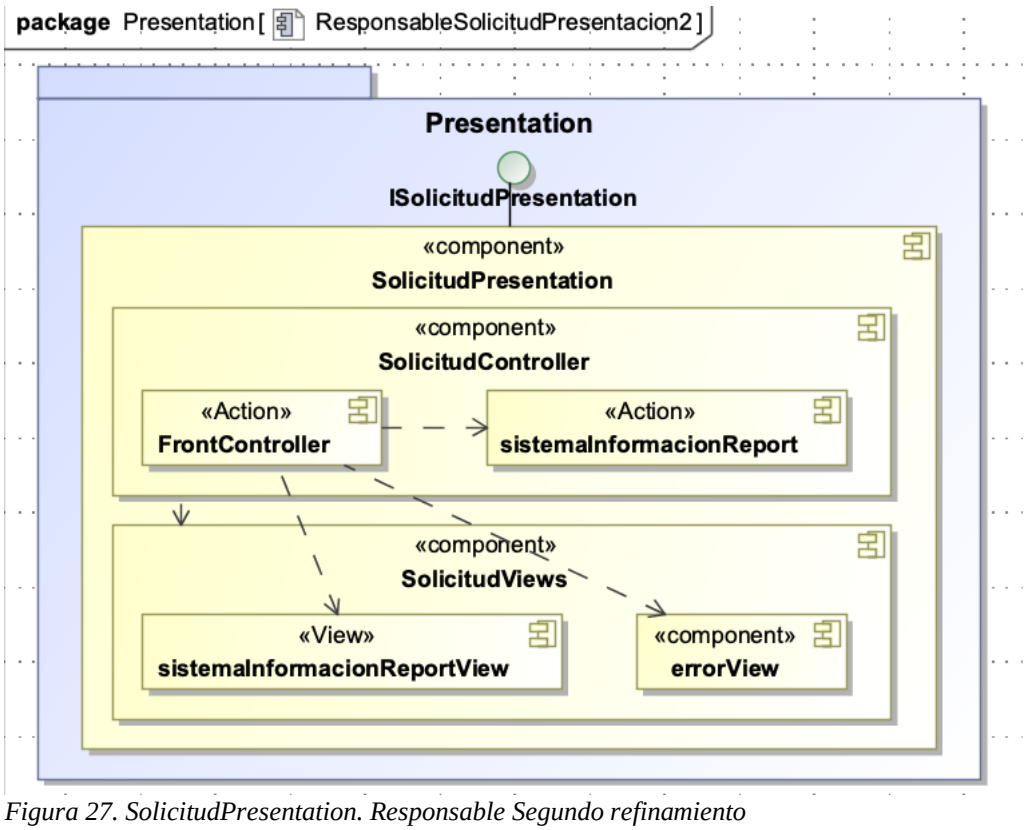


Figura 27. SolicitudPresentation. Responsable Segundo refinamiento

Como resultado de este segundo refinamiento, para el solicitante obtenemos las siguientes acciones y vistas:

- Acciones:
  - sistemaInformaciónReport: Generar informe de un sistema de informción del responsable del tratamiento logado.
- Vistas:
  - sistemaInformacionReportView. Vista con información estadística de las solicitudes presentadas (pendientes de tramitar, en tramitación y resueltas) así como un listado de la productividad de los tramitadores del sistema.

Perfil J2EE

Solicitante

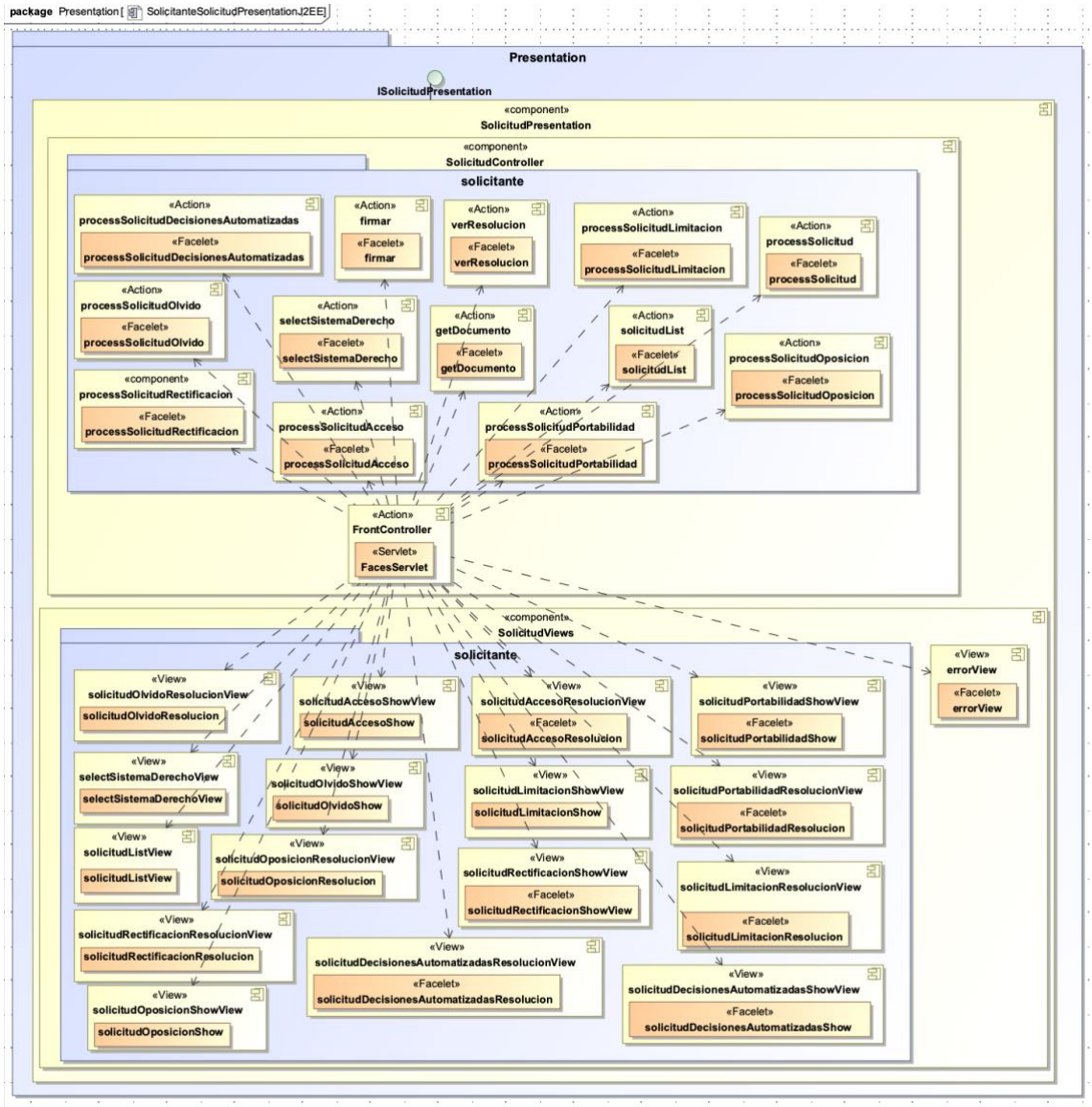


Figura 28. SolicitudPresentation. Solicitante Perfil J2EE

Tramitador

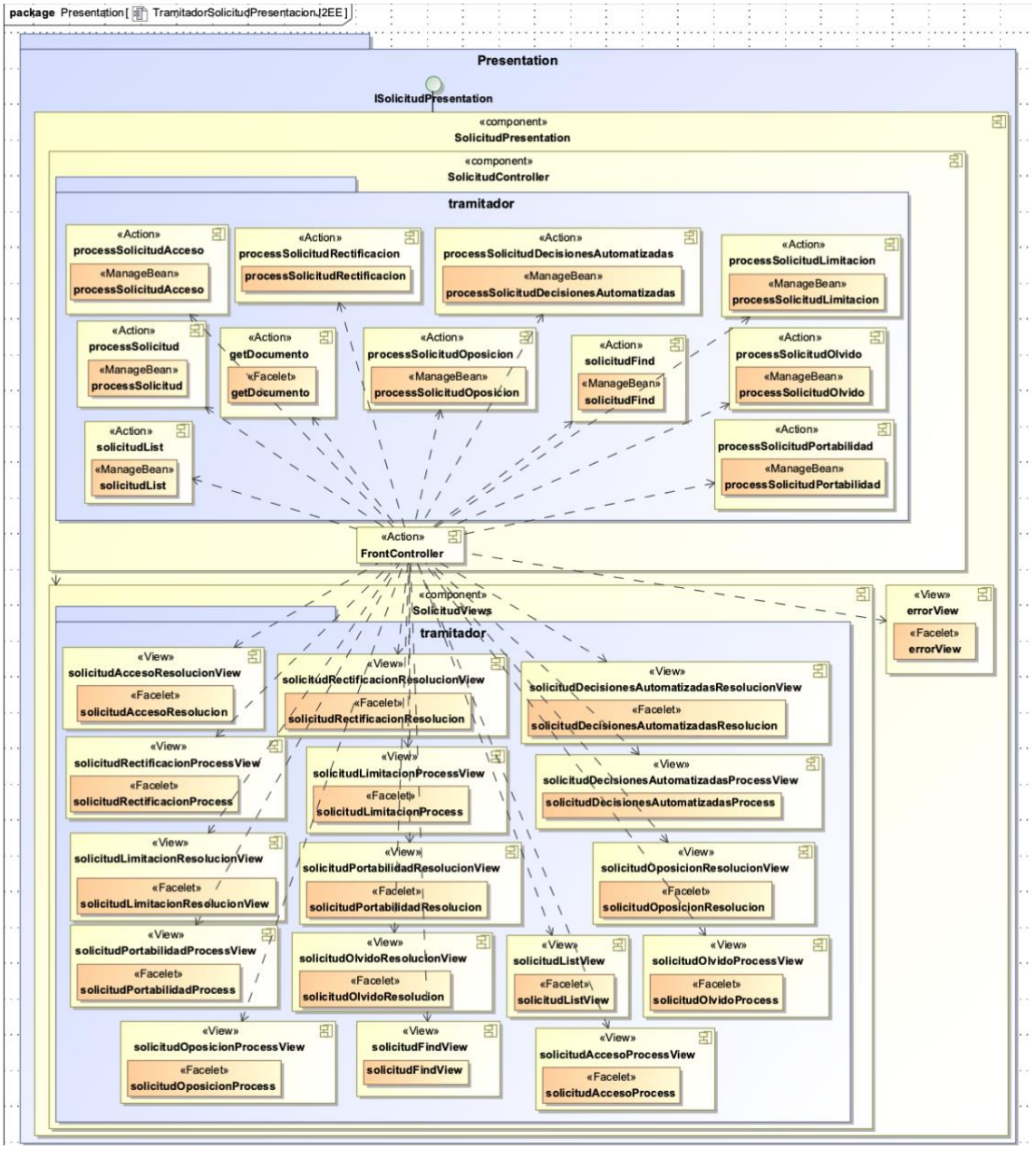


Figura 29. SolicitudPresentation. Tramitador Perfil J2EE

Responsable

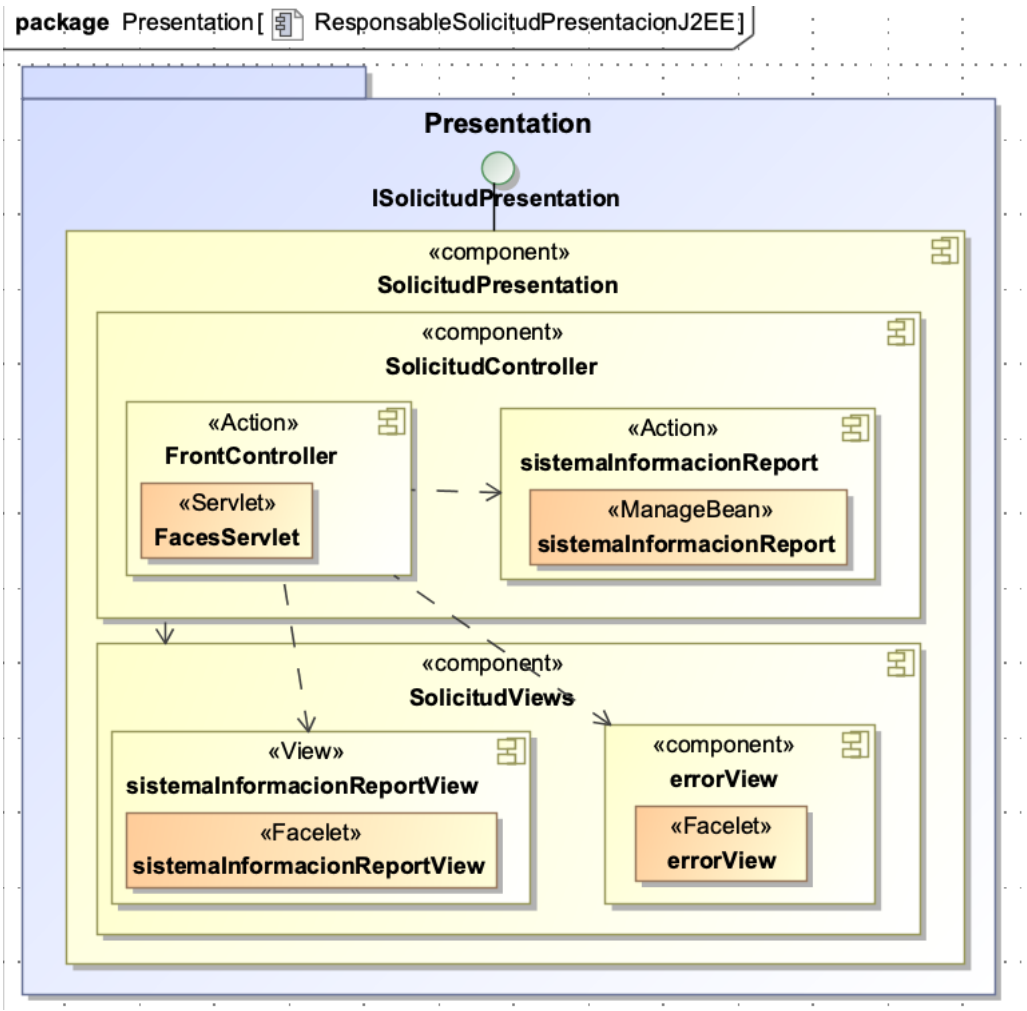


Figura 30. SolicitudPresentation. Responsable Perfil J2EE

3.3.2 Negocio

El diseño de los componentes de la capa de negocio se basará en el patrón estructural Facade con el fin de centralizar en un solo interface las comunicaciones entre capas, resultando un primer diagrama (**Primer refinamiento**) listo para aplicar a continuación el perfil J2EE.

Se decide usar los componentes de la especificación J2EE, Enterprise Java Beans (EJB) Stateless, ya que las operaciones a realizar son síncronas y sin estado. Además, podemos delegar al contenedor J2EE la gestión de las transacciones, el acceso remoto y la seguridad que nos proporciona fácilmente. El acceso a los EJB's podrá realizarse tanto remotamente como de manera local, por lo que definiré dos interfaces, local (<<EJBLocalInterface>>) y remoto (<<EJBRemoteInterface>>).
Para el componente responsable de la comunicación con los sistemas de información externos gestionados por eRGPD que disponen de web service SOAP (fuera del alcance de este proyecto eRGPD, se implementará una versión dummy), encargado de la tramitación síncrona de solicitudes, generaremos un cliente implementado con Java API for XML Web Service (JAXWS) de la especificación J2EE (<<WebServiceClient>>).

Con estas decisiones de diseño, aplicando el **perfil J2EE** a la capa de negocio, obtenemos para cada uno de los componentes (Profile, Seguridad, Solicitudes y

SystemAdministration) el diagrama definitivo ya dependiente de la tecnología seleccionada.
Los diagramas resultantes son los siguientes:

ProfileBusiness

Primer Refinamiento

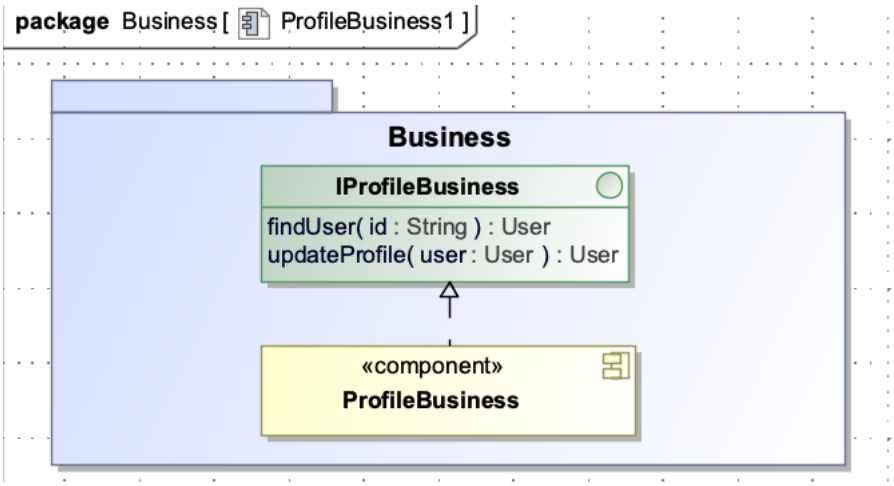


Figura 31. ProfileBusiness. Primer Refinamiento

Perfil J2EE

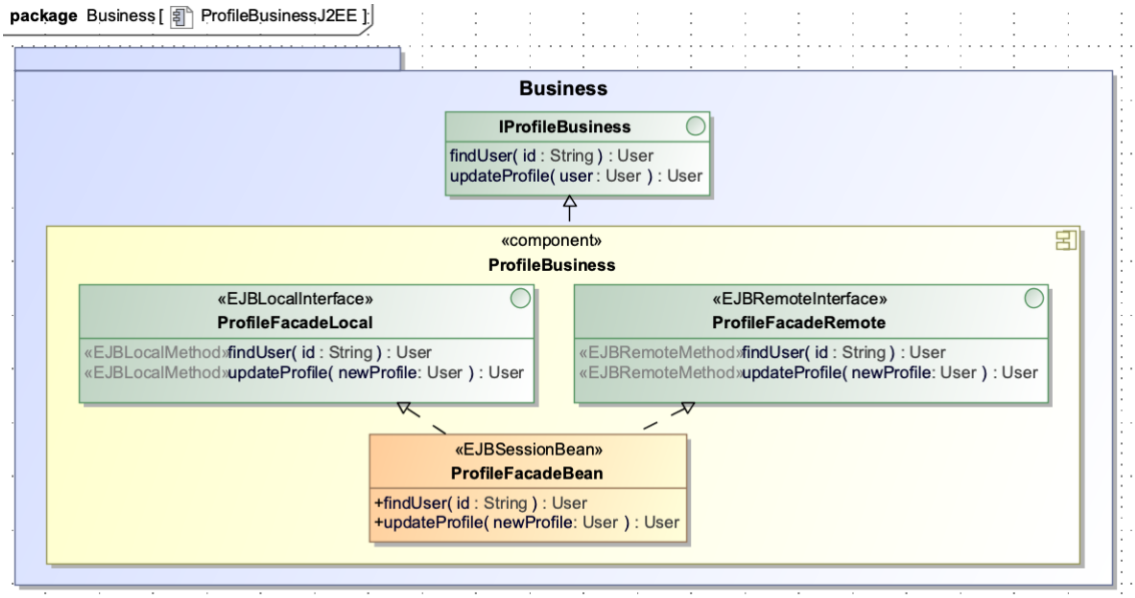


Figura 32. ProfileBusiness. Perfil J2EE

SeguridadBusiness

Primer Refinamiento

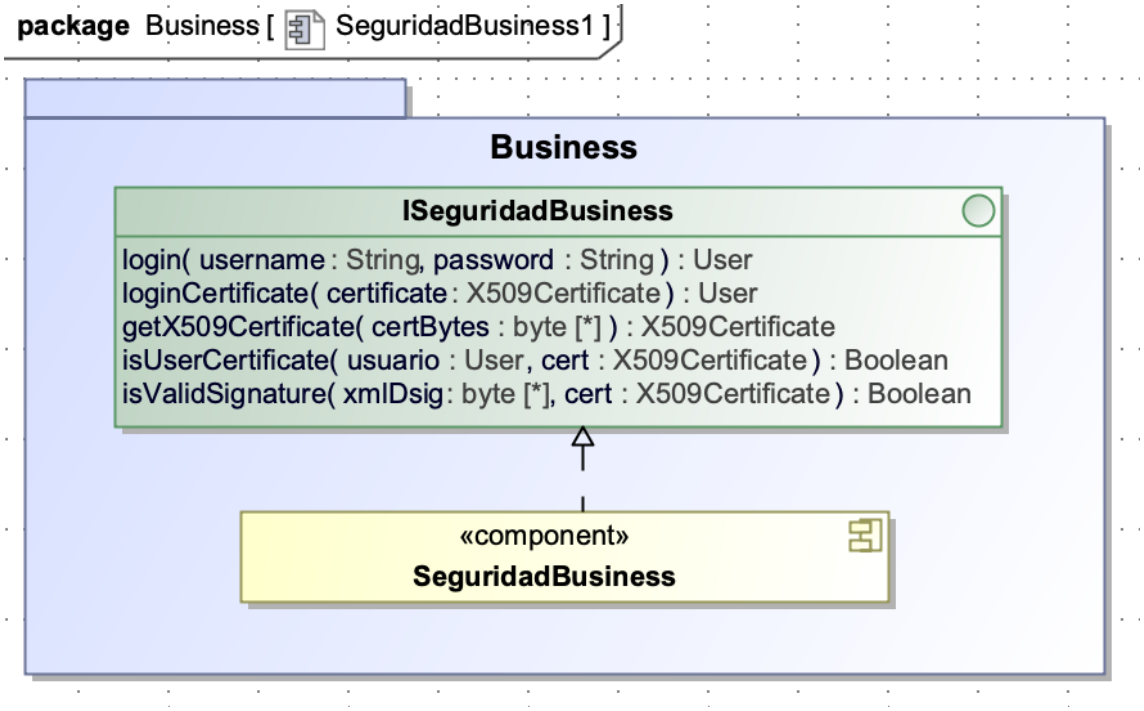


Figura 33. SeguridadBusiness. Primer refinamiento

Perfil J2EE

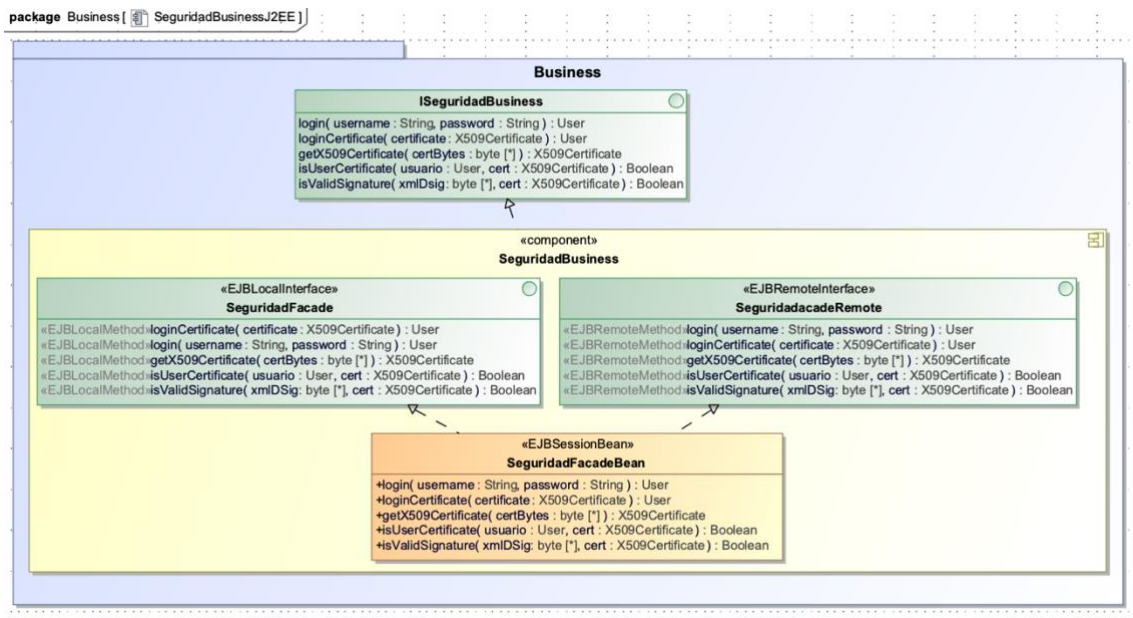


Figura 34. SeguridadBusiness. Perfil J2EE

SystemAdministrationBusiness

Primer Refinamiento

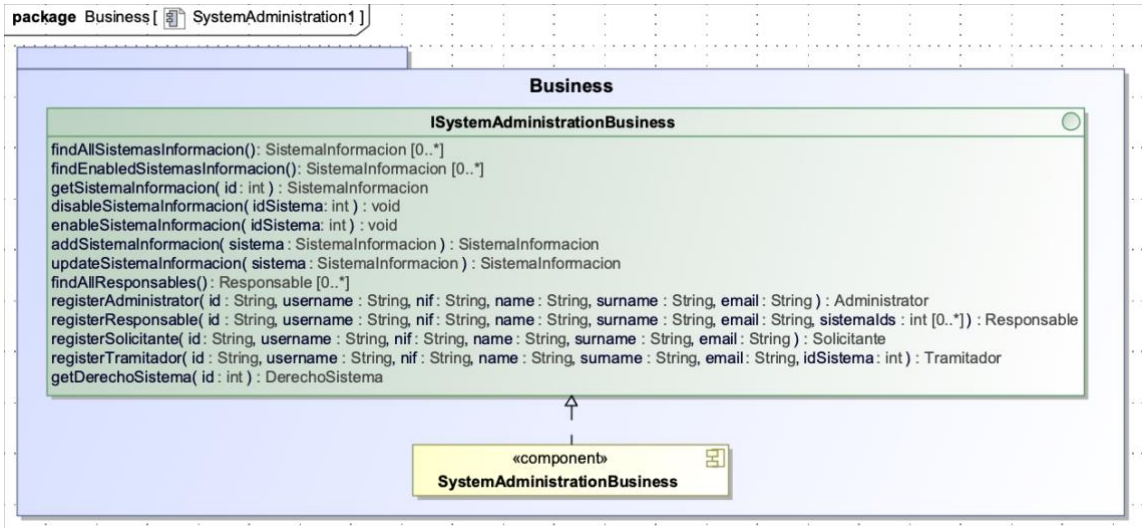


Figura 35. SystemAdministrationBusiness. Primer refinamiento

Perfil J2EE

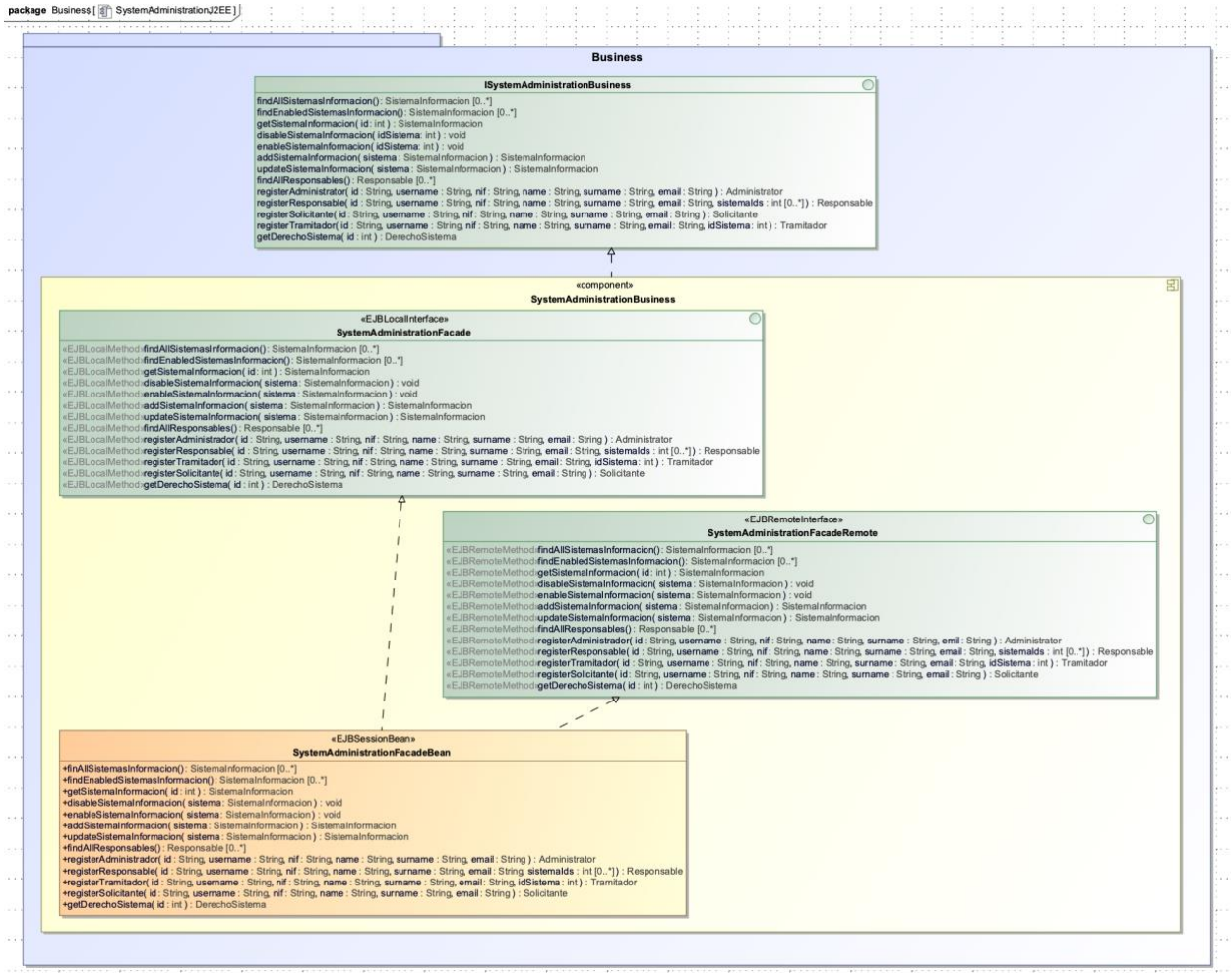


Figura 36. SystemAdministrationBusiness. Perfil J2EE

SolicitudesBusiness

Primer Refinamiento

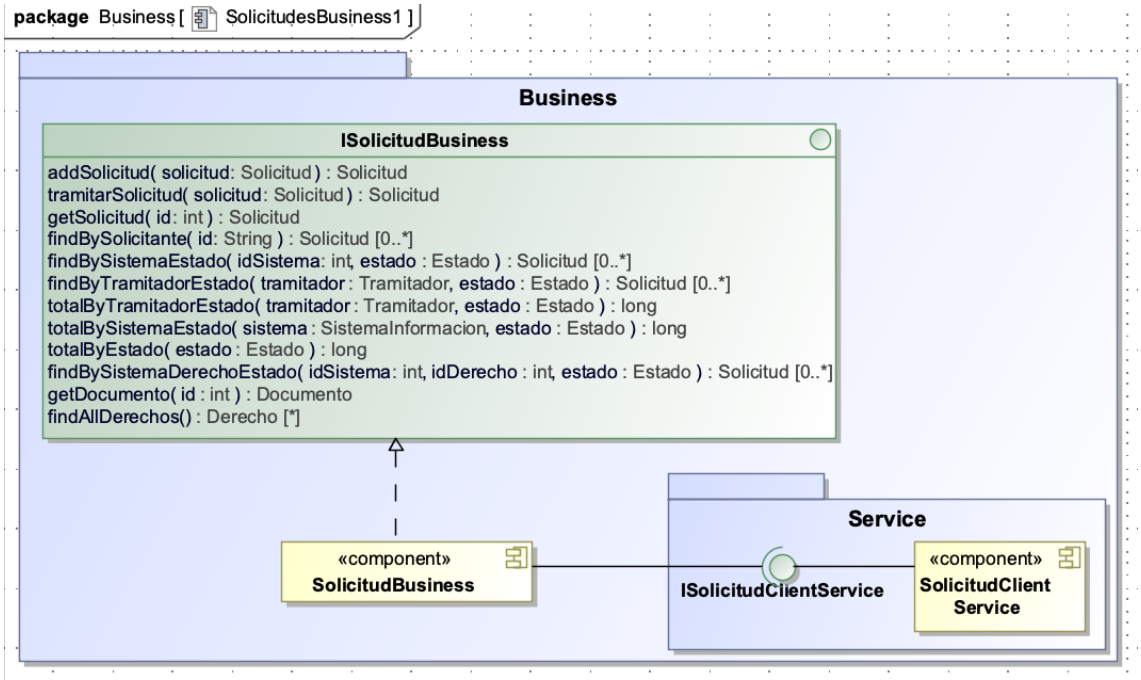


Figura 37. SolicitudesBusiness. Primer refinamiento

Perfil J2EE

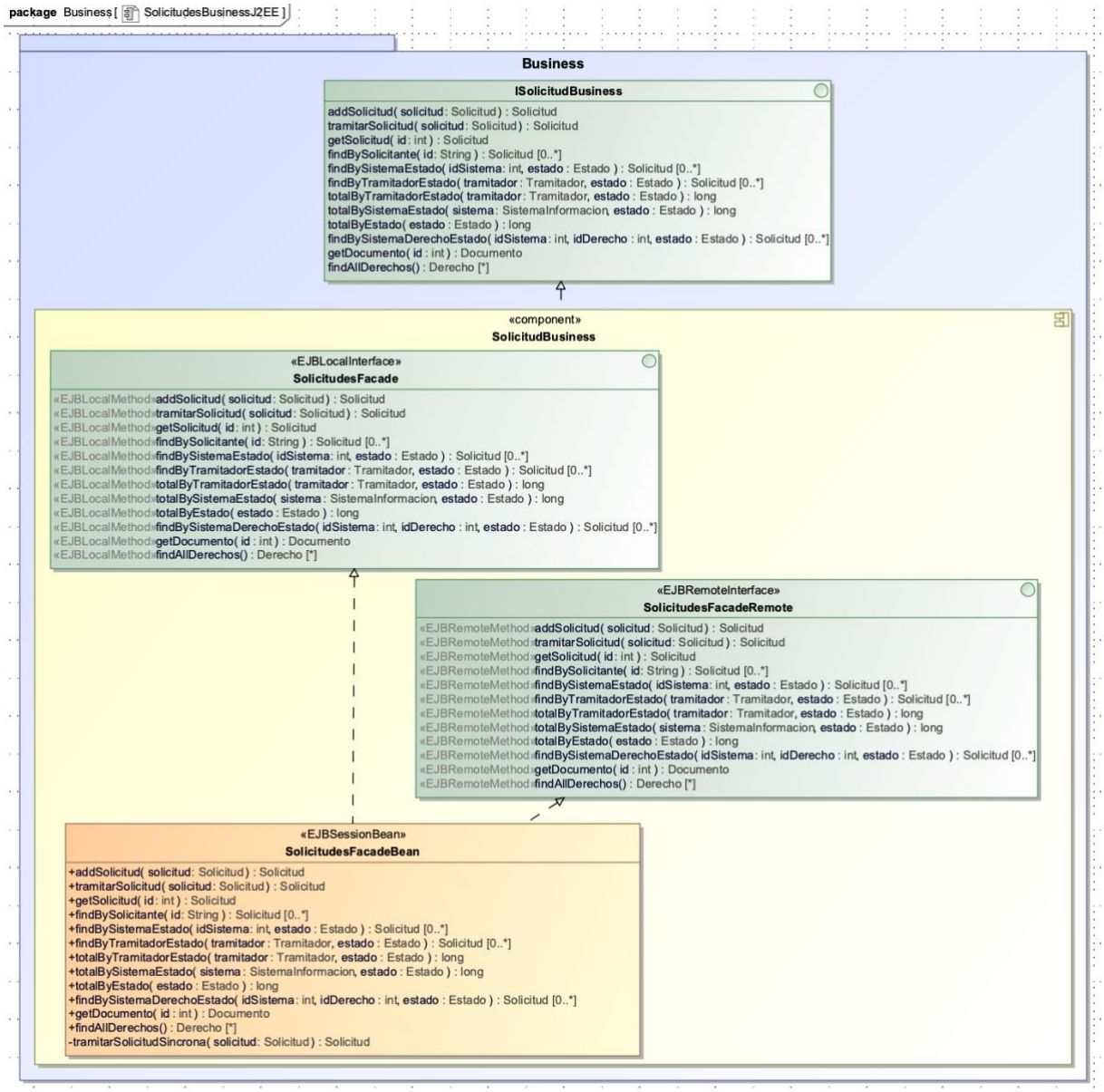


Figura 38. SolicitudesBusiness. Perfil J2EE

Como se puede comprobar, incluimos un método privado "tramitarSolicitudSincrona", que será invocado por el método del interface "tramitarSolicitud" cuando el tipo de ejecución sea síncrono para procesar las solicitudes a través del componente SolicitudClientService.

SolicitudClientService

Primer Refinamiento

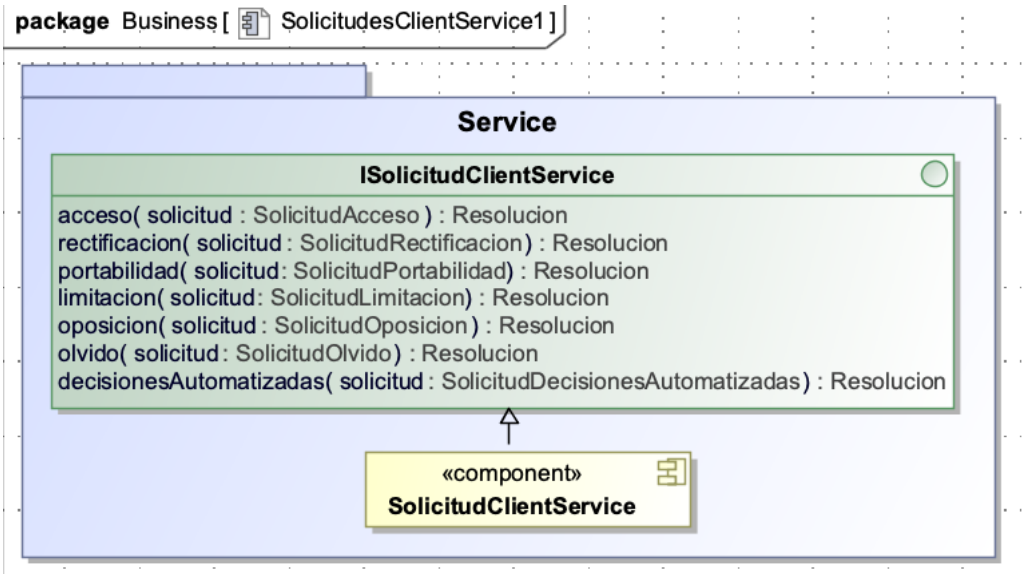


Figura 39. SolicitudesService. Primer Refinamiento

Perfil J2EE

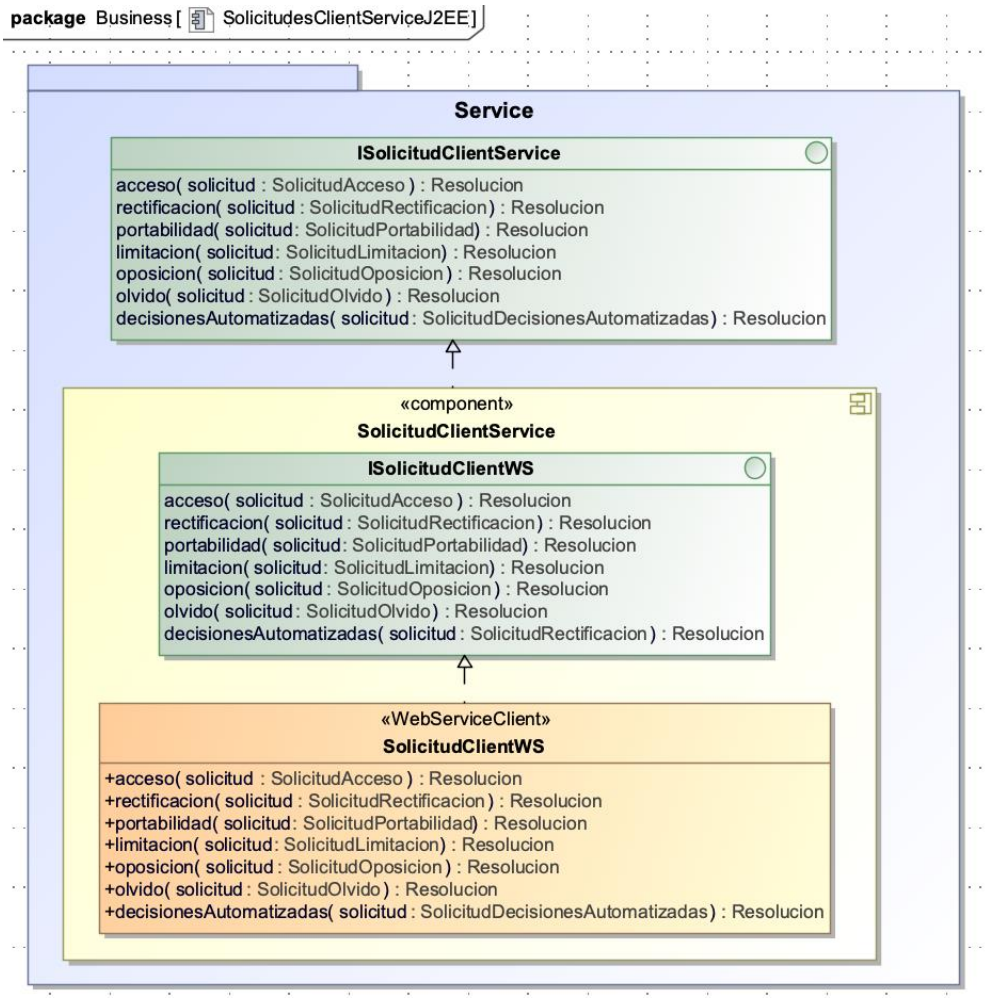


Figura 40. SolicitudesService. Perfil J2EE

3.3.3 Integración

Teniendo en cuenta las siguientes decisiones de diseño:

- Uso de una base de datos relacional para gestionar la información del sistema eRGPD.
- El acceso a la capa de persistencia se implementará de manera local por motivos de eficiencia, pero se desea diseñar el sistema abierto a un posible acceso remoto con el menor impacto en el diseño de los componentes.
- El modelo de aplicación J2EE promueve el uso de Java Persistence API (JPA) (independencia de la implementación ORM específica del servidor de aplicaciones donde despleguemos eRGPD) para la capa de integración con bases de datos relacionales, como es el caso que nos ocupa.

Se decide implementar la interface de los componentes de integración con EJB's stateless, defino el interface local (<<EJBLocalInterface>>), y dejo la posibilidad sin coste a publicar una interface remota del componente de acceso a datos en caso necesario. Aplicaremos el patrón de diseño Data Access Object (DAO), cabe señalar que es en la capa de negocio donde se gestionan las transacciones, y que estos EJB's de integración se unen a la transacción abierta. Y por último usaré JPA para el acceso a la base de datos, y su lenguaje estándar de consultas Java Persistence Query Language (JPQL), expresando las consultas en base a nuestras clases del dominio y sus relaciones, permitiéndonos abstraernos del gestor de base de datos elegido, lo que redunda en uno de los requisitos del sistema, su portabilidad a otros gestores de base de datos.
Solo se mostrarán en los diagramas, las clases del dominio (<<JPAEntity>>) que tengan dependencia directa.
Los diagramas resultantes tras aplicar el perfil J2EE a los componentes de acceso a datos son los siguientes:

ProfileIntegration

Perfil J2EE

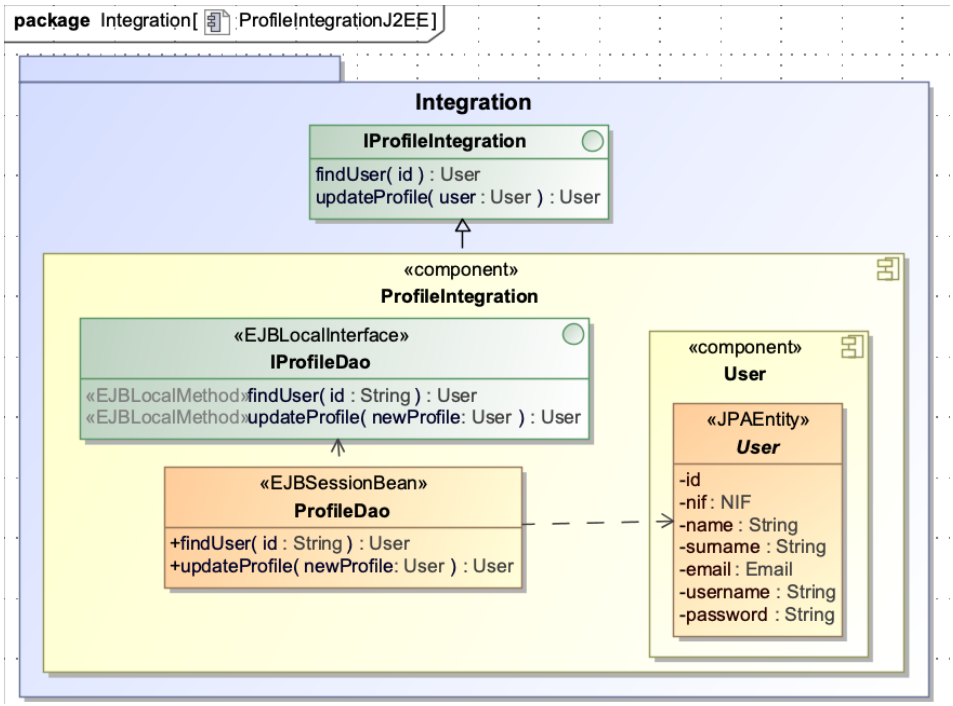


Figura 41. ProfileIntegration. Primer refinamiento

SeguridadIntegration

Perfil J2EE

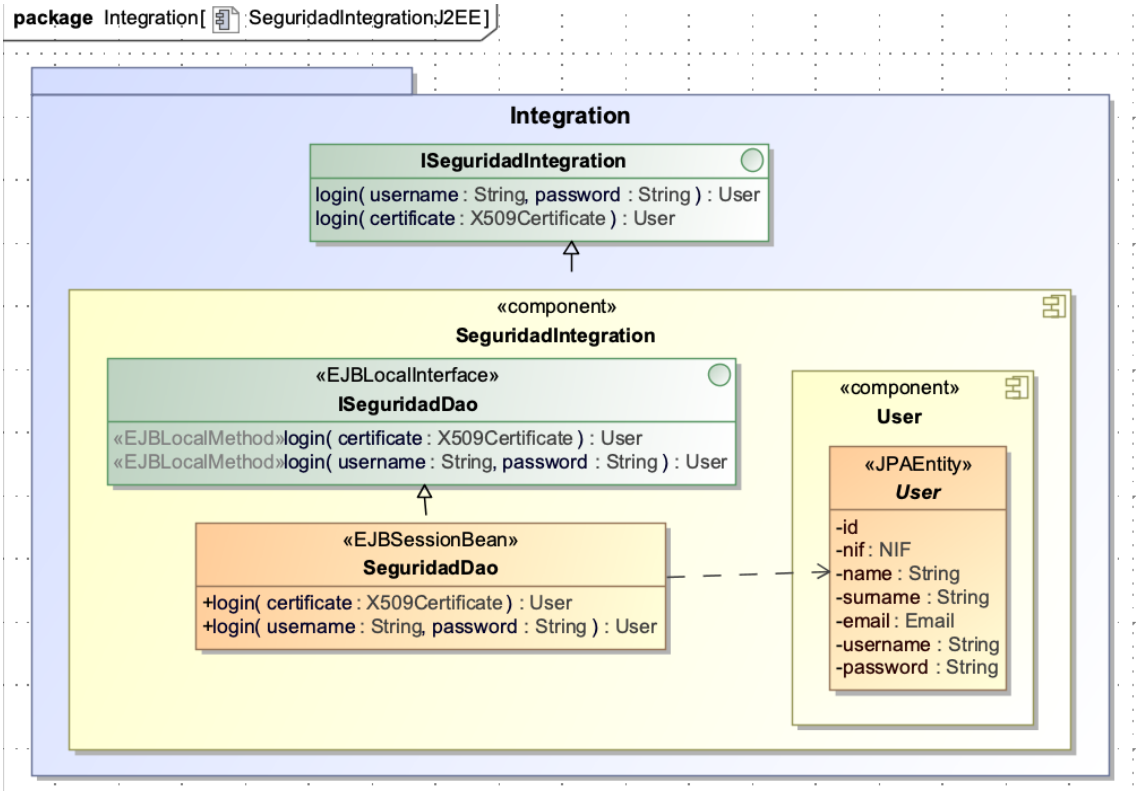


Figura 42. ProfileIntegration. Perfil J2EE

SystemInformationIntegration

Perfil J2EE

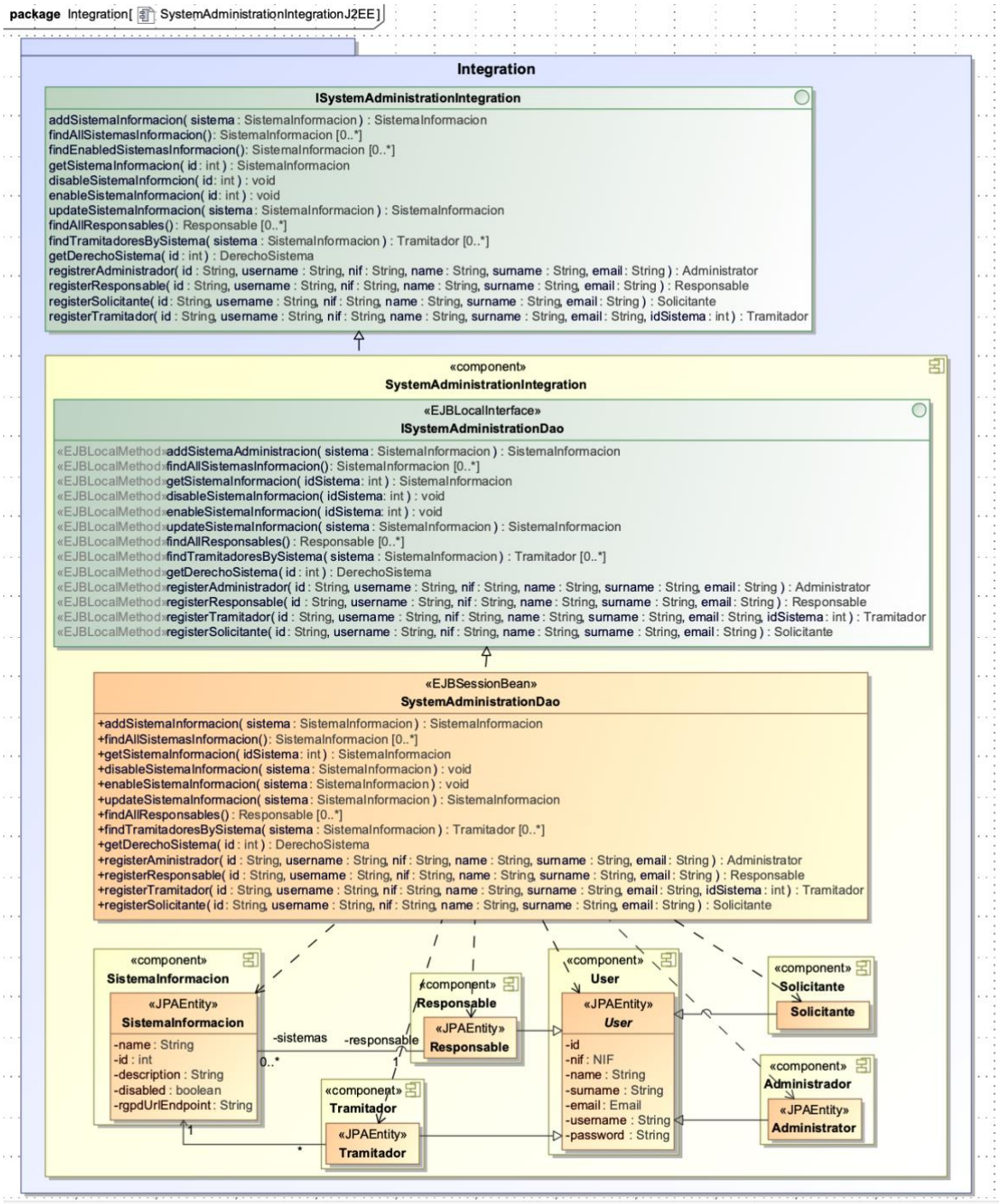


Figura 43. SystemAdministrationIntegration. Primer refinamiento

SolicitudesIntegration

Perfil J2EE

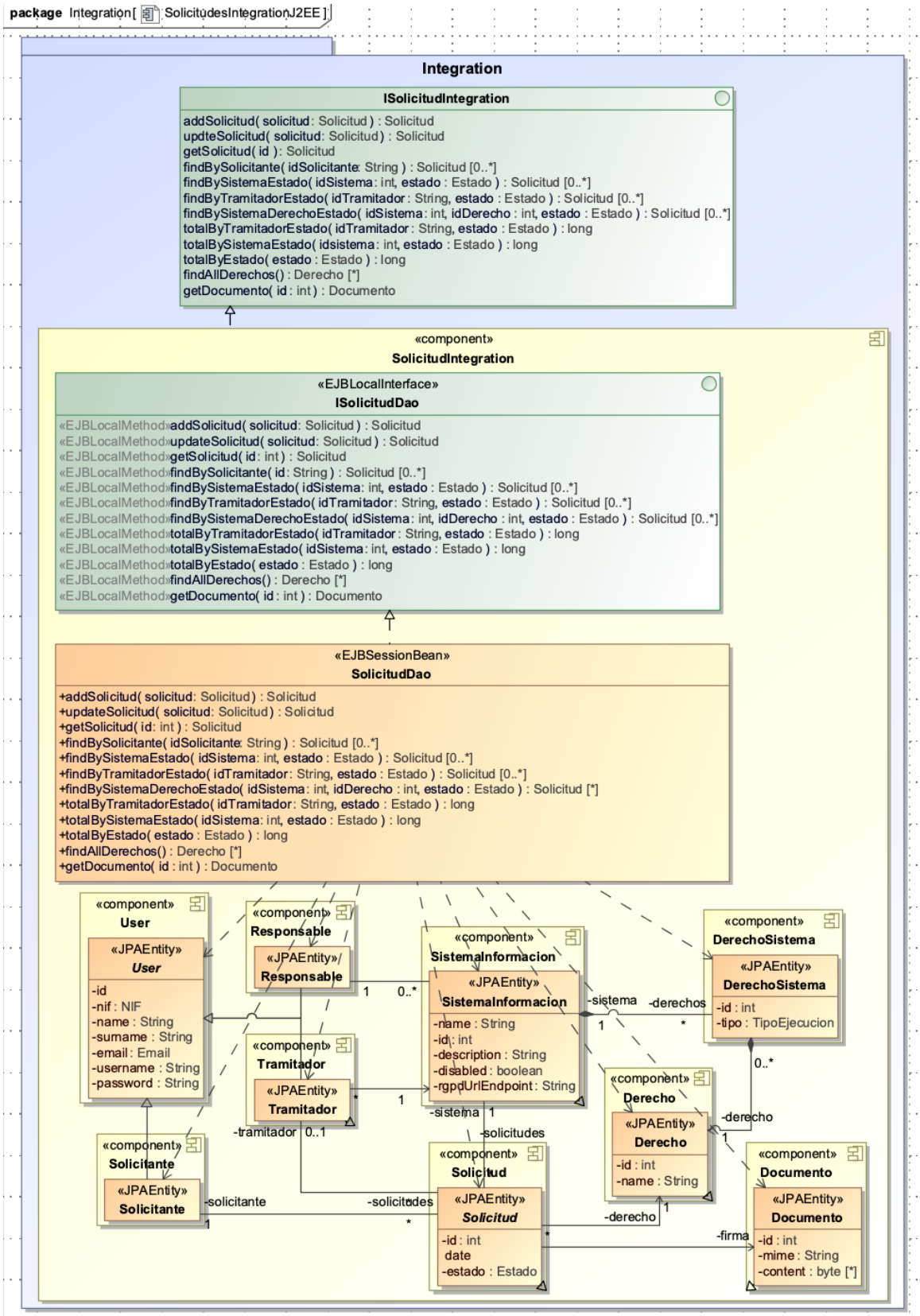


Figura 44. SystemAdministrationIntegration. Perfil J2EE

3.4 Diagrama Relacional

Ateniéndome a la especificación del modelo de clases del dominio, a continuación, muestro el diagrama relacional detallado de la base de datos:

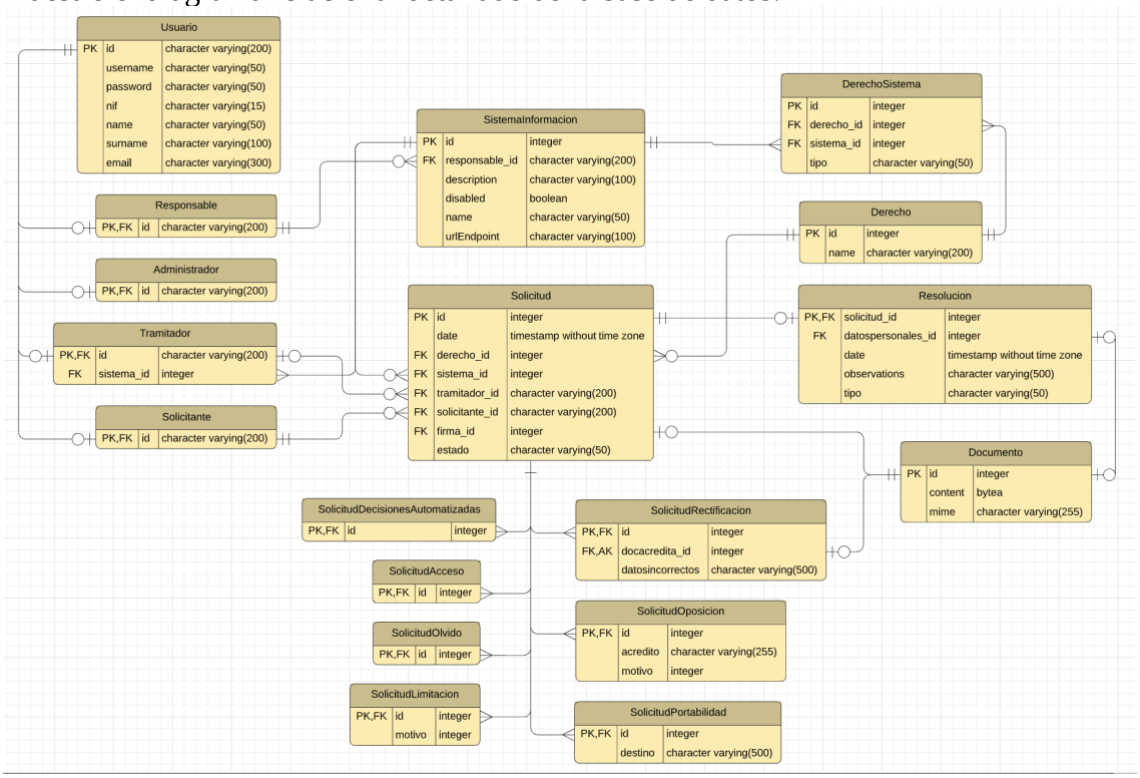


Figura 45. Diagrama relacional

3.5 Prototipo. Modelo de Pantallas

3.5.1 Usuario no logado

Home

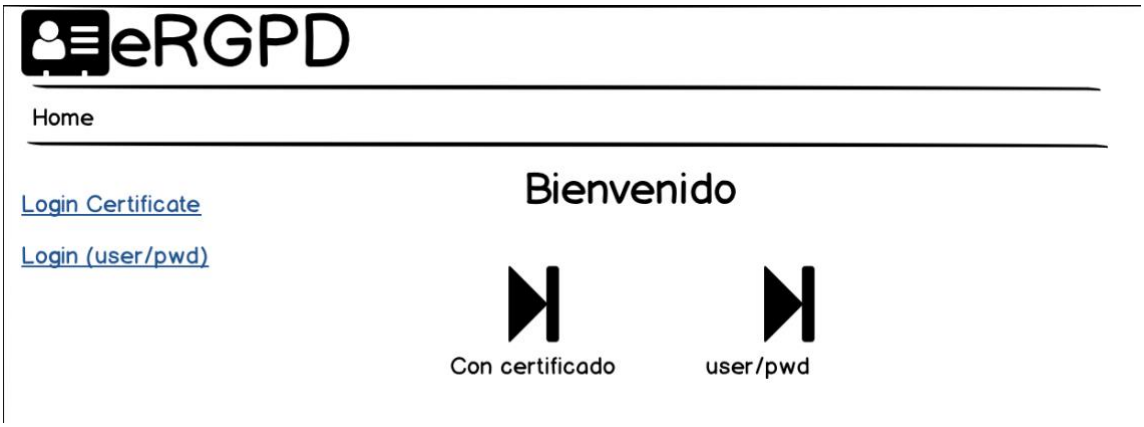


Figura 46. Pantalla Home

Login user/pwd

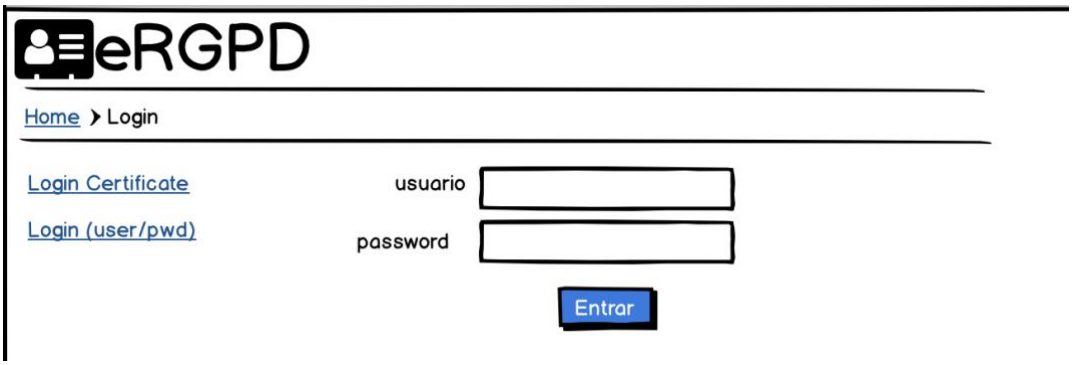


Figura 47. Pantalla Login user/pwd

3.5.2 Usuario logado

Mi Cuenta

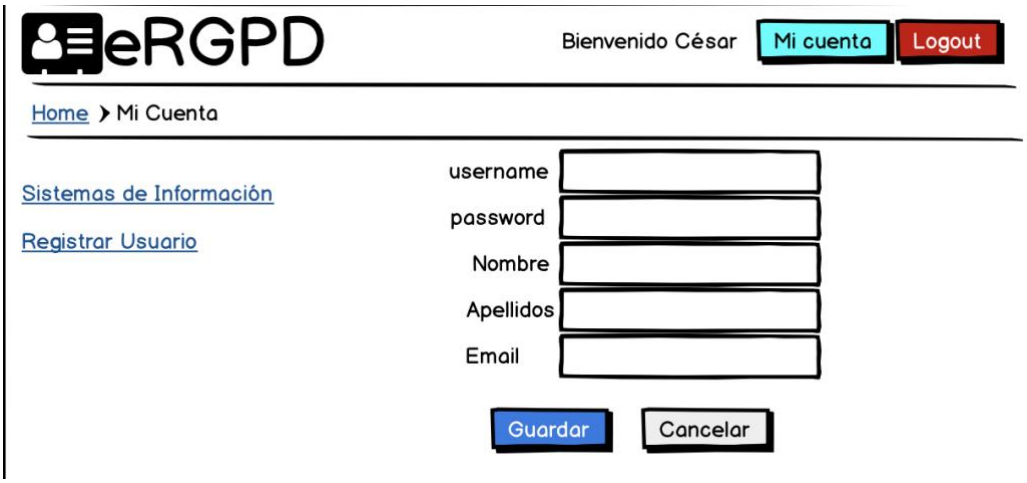


Figura 48. Pantalla Mi Cuenta

3.5.3 Administrador

Listado de Sistemas de Información

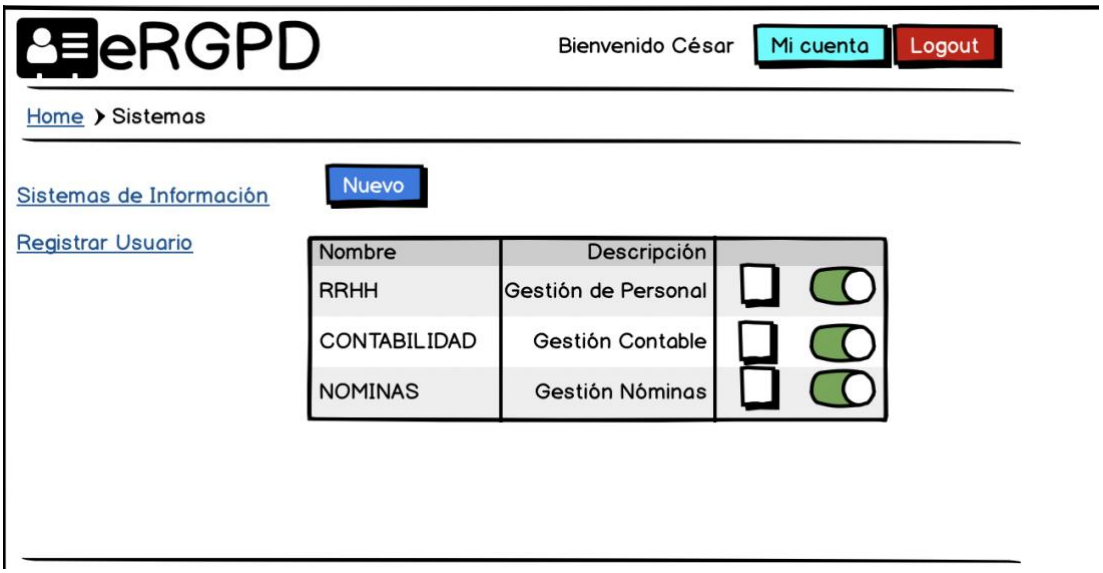


Figura 49. Pantalla Administrador. Listado Sistemas de información

Nuevo Sistema de Información

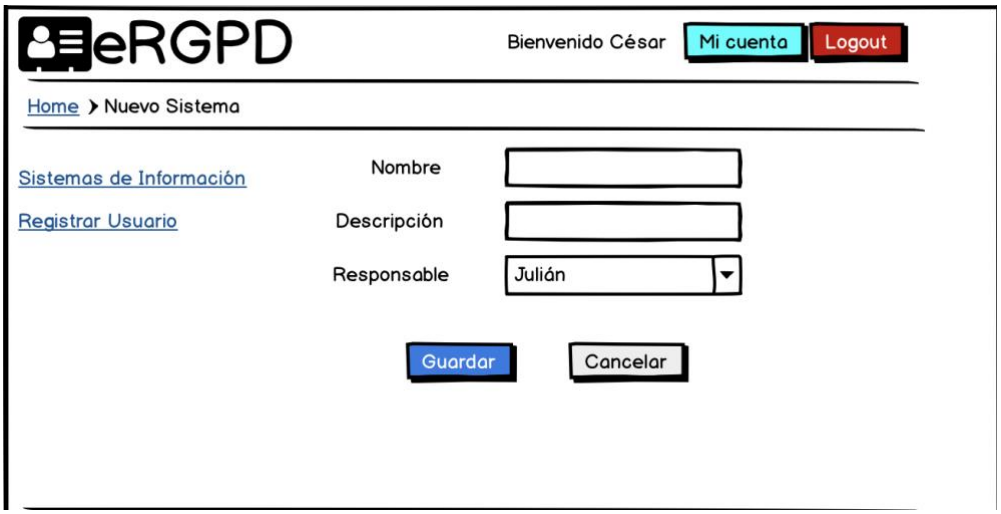


Figura 50. Pantalla Administrador. Nuevo Sistema de información

Editar Sistema de Información

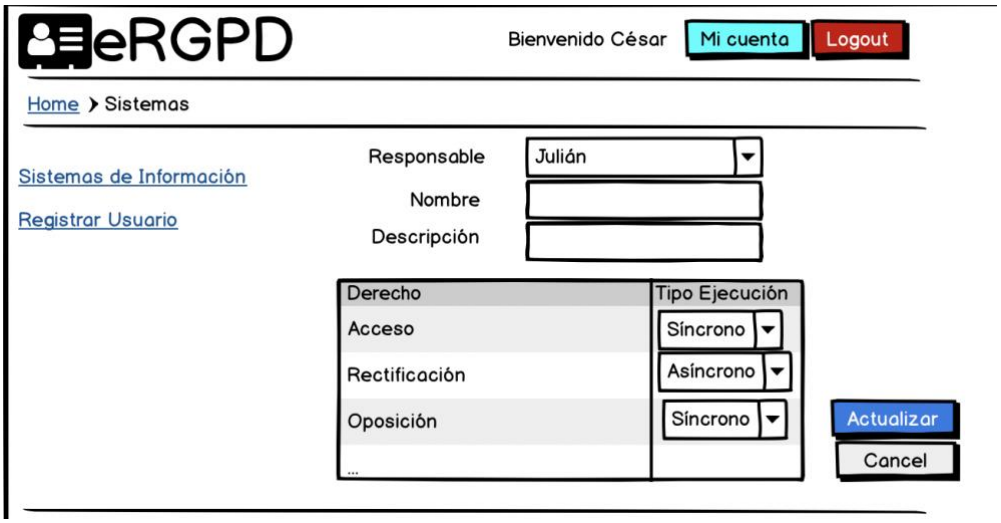


Figura 51. Pantalla Administrador. Editar Sistema de información

Registrar usuario

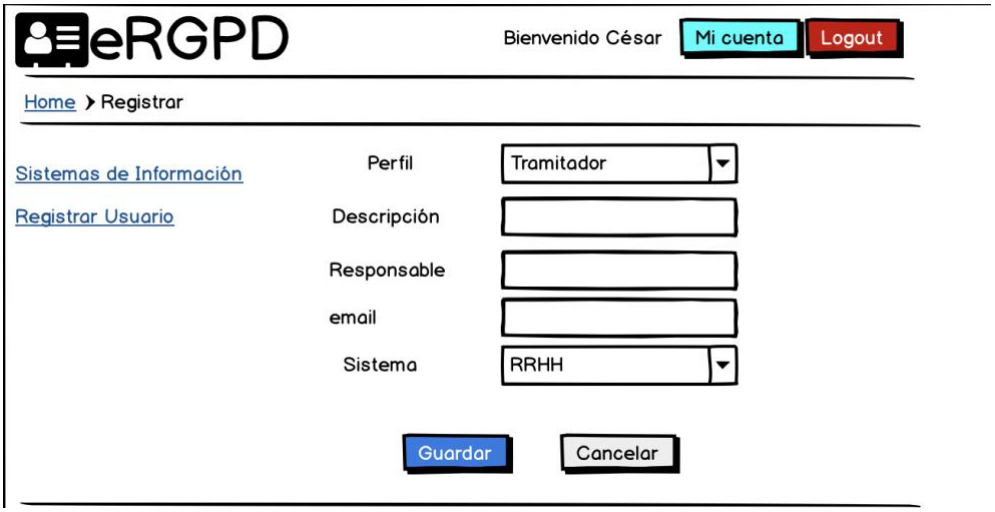


Figura 52. Pantalla Administrador. Registrar usuario

3.5.4 Responsable

Generar Informe

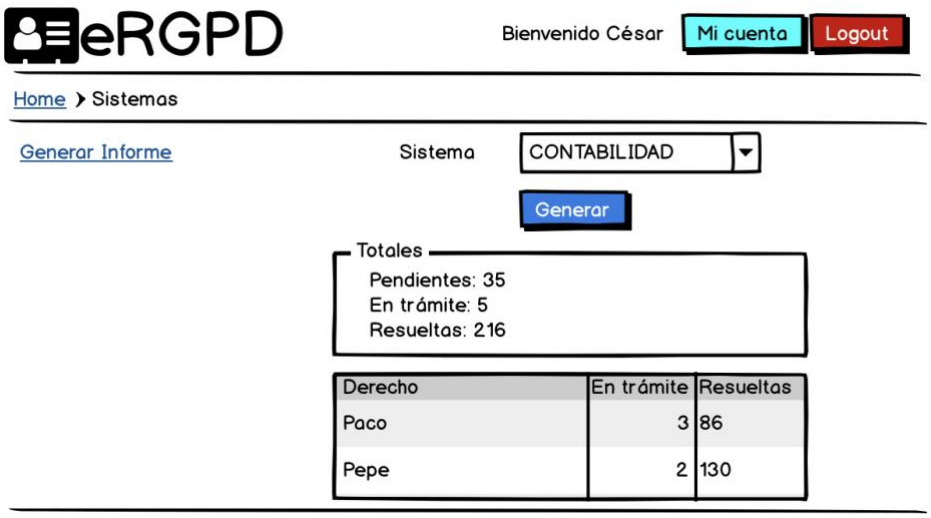


Figura 53. Pantalla Responsable. Generar Informe

3.5.5 Tramitador

Buscador Solicitudes

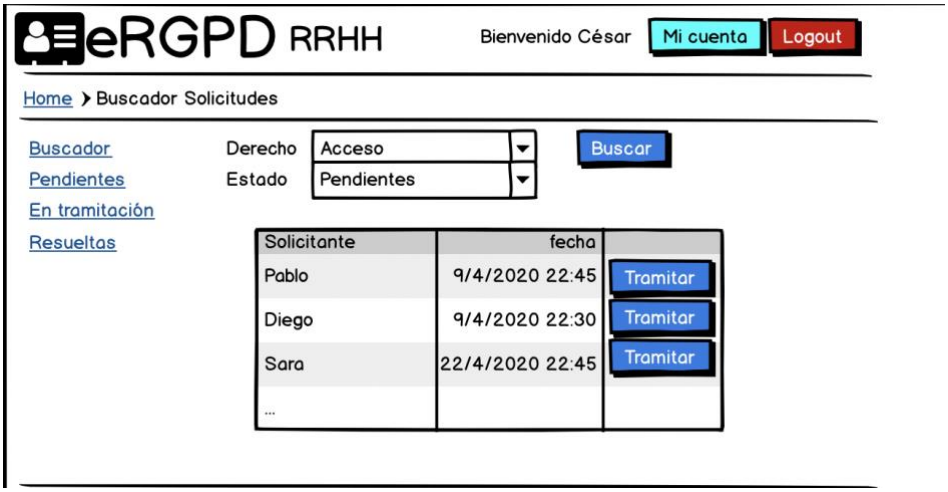


Figura 54. Pantalla Tramitador. Buscador Solicitudes

Solicitudes Pendientes/En tramitación

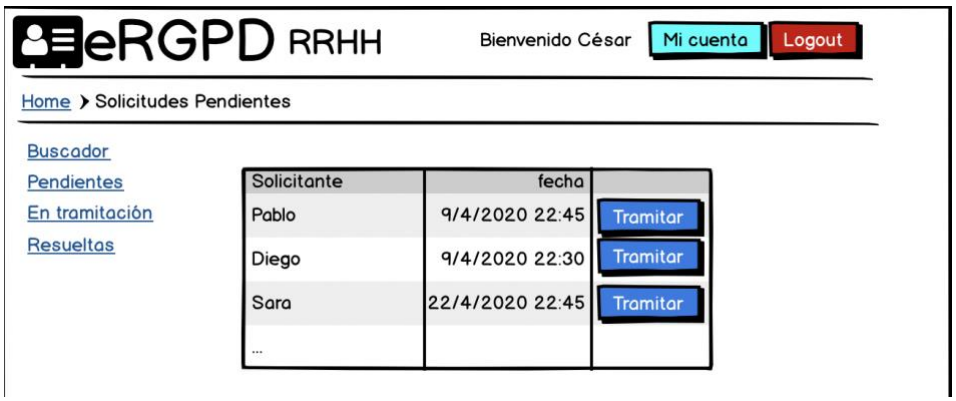


Figura 55. Pantalla Tramitador. Solicitudes Pendientes/En tramitación

Solicitudes Resueltas

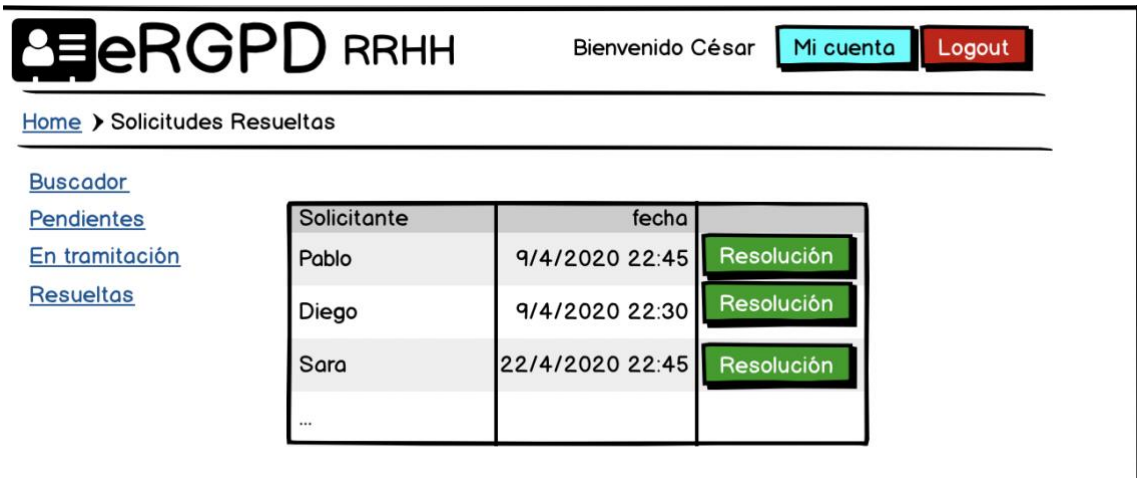


Figura 56. Pantalla Tramitador. Solicitudes Resueltas

Tramitar

Diseño solo la pantalla de la tramitación del derecho de oposición por economía de espacio, siendo para el resto es similar, lo único que varía son los datos de la solicitud, dependiendo del derecho solicitado se introducen unos valores u otros. Los campos de tramitación también se ajustan a lo necesario para resolver el derecho solicitado.

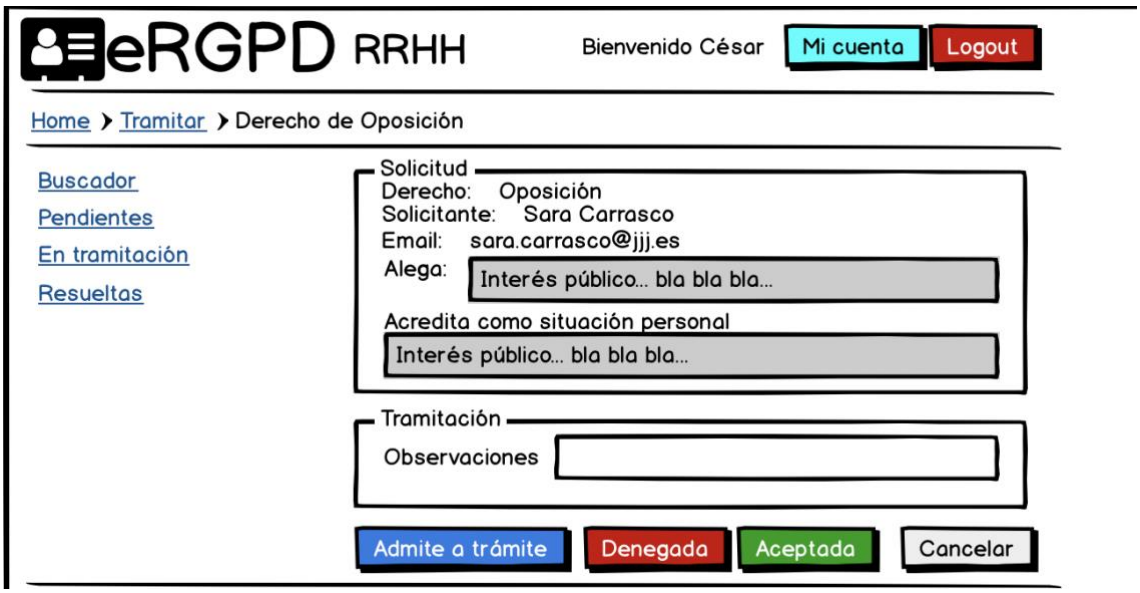


Figura 57. Pantalla Tramitador. Tramitar

3.5.6 Solicitante

Seleccionar Sistema y Derecho

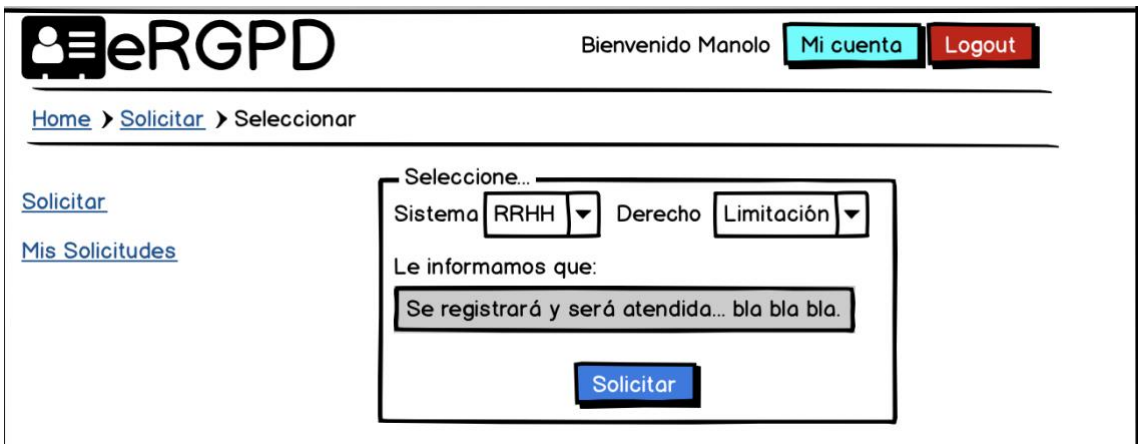


Figura 58. Pantalla Solicitante. Seleccionar Sistema y Derecho

Solicitar Derecho de <Derecho>

Diseño solo la pantalla de la solicitud del derecho de rectificación, por economía de espacio, siendo para el resto similar, lo único que hay que personalizar son los campos de del formulario de solicitud, dependientes del derecho ejercido.

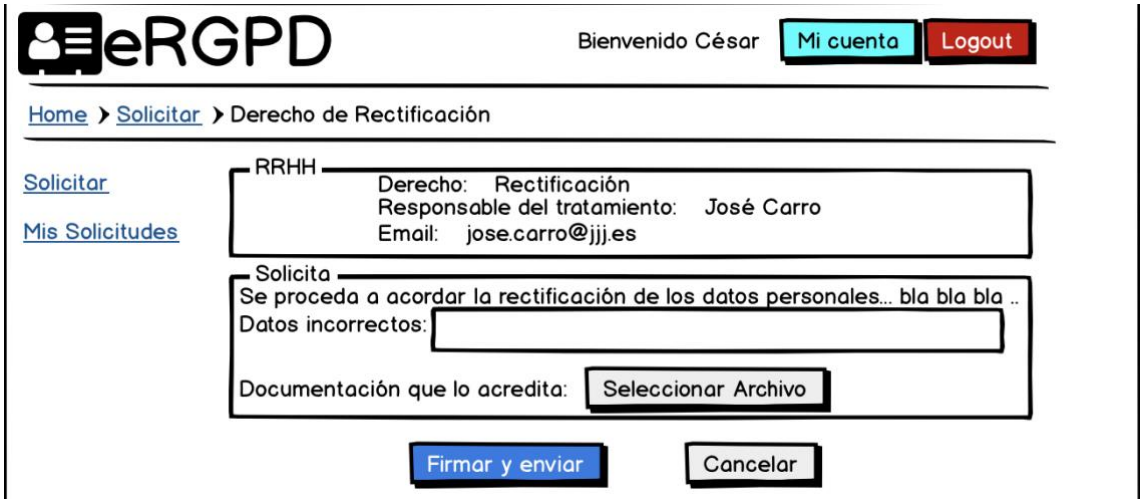


Figura 59. Pantalla Solicitante. Solicitar Derecho

Mis Solicitudes

Figura 60. Pantalla Solicitante. Mis Solicitudes

Resolución

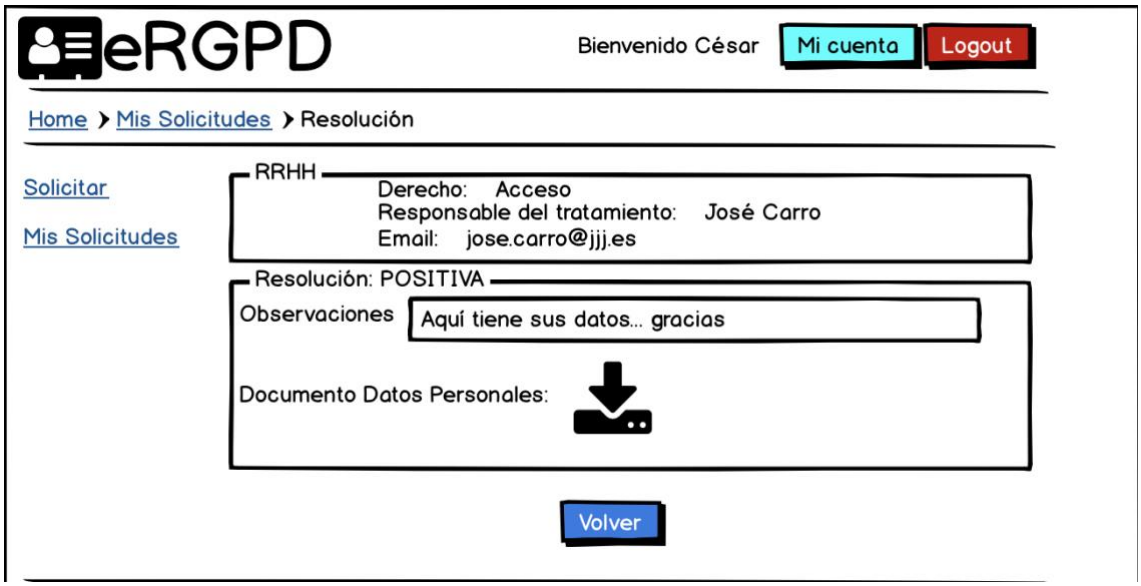


Figura 61. Pantalla Solicitante. Ver Resolución

3.6 Entorno Tecnológico del Sistema

A continuación, una vez verificados la calidad técnica del diseño y su coherencia, se define el entorno tecnológico del sistema que de soporte a la arquitectura del sistema que hemos descrito.

- Navegador web: Chrome (certificado personal FNMT importado)
- Aplicación firma electrónica: Autofirma
- JavaSE: Java 1.8.0_202
- Gestor Base de datos relacional: PostgreSQL 10.x
- Servidor de Aplicaciones J2EE: Wildfly-18.0.1.Final

3.7 Seguridad del Sistema

La seguridad es uno de los factores más importantes del sistema eRGPD. Debemos realizar un análisis de riesgos de la seguridad de la arquitectura tecnológica de la solución propuesta, para ello, debemos establecer unos niveles en las características de seguridad (ACID) de autenticación, confidencialidad, integridad, disponibilidad y no repudio, adoptando medidas de seguridad proporcionales al riesgo establecido.

3.7.1 Autenticación

El nivel de autenticación debe ser Alto. Dependiendo del sistema de información sobre el que estemos ejerciendo un derecho, los datos personales que trata pueden estar clasificados según el RGPD como especialmente protegidos (ideología, religión, salud, infracciones penales, …). Para garantizar este nivel de seguridad, solicitaremos al usuario del sistema que se autentique con su certificado personal.

3.7.2 Confidencialidad

El nivel de confidencialidad debe ser Alto. Es un requisito del sistema que solo el usuario pueda acceder a sus datos personales. Para garantizarlo, además de identificar al usuario de la aplicación con su certificado, la transmisión de datos debe ser cifrada, usaremos el protocolo de comunicaciones https configurando el acceso a nuestro servidor J2EE con protocolo TLSv1.2. Crearemos un almacén de certificados (server.keystore) para almacenar el certificado SSL de servidor, y un segundo almacén para los certificados de confianza (client.truststore), donde almacenaremos el certifica raíz de la CA de la FNMT (emisor de los certificados personales con los que nos autenticamos en el sistema). Para más información, ver anexo 1, apartado 9.2.1.

3.7.3 Integridad

El nivel de integridad debe ser Alto. Debemos garantizar no solo la integridad tanto de las comunicaciones (a través del protocolo https), si no también el de las solicitudes presentadas. Para ello, el solicitante las firmará electrónicamente con su certificado personal usando la aplicación AutoFirma, generando un XMLDSig, que validaremos en el componente que procesa las solicitudes, de tal forma que cualquier modificación de la solicitud provoque que la firma no sea válida.

3.7.4 Disponibilidad

La arquitectura del sistema eRGPD es altamente escalable, no obstante, dependerá del servicio ofrecido por la organización donde implantemos el sistema, lo que definirá el nivel de disponibilidad del sistema bajo, medio o alto.

3.7.5 No Repudio

Al igual que la integridad, el sistema garantiza el no repudio a través de la firma electrónica de las solicitudes con el certificado personal del solicitante, ya que la solicitud y su firma digital asociada probará de manera efectiva la identidad del usuario que presentó la solicitud.

3.8 Decisiones de Diseño Seguridad

3.8.1 Autenticación

En la especificación Java EE 8 se incluye la nueva interface Java EE Security API 1.0, como en el resto del proyecto, se ha decidido aprovechar las capacidades de la especificación estándar con el fin de garantizar la portabilidad del proyecto a cualquier servidor de aplicaciones con certificación Java EE 8.
Para la autenticación por tanto en nuestro sistema eRGPD, implementamos la interfaz `javax.security.enterprise.authentication.mechanism.http.HttpAuthenticationMechanism`, validando cada petición de usuario en el método `validateRequest`, en caso de no estar autenticado en el sistema, se obtendrá de la request, el usuario/password o bien el certificado personal `X509Certificate` para identificarlo en el sistema con los métodos `login` o `loginCertificate` del componente de la capa de negocio SeguridadBusiness, que cargará la información del usuario así como el role/perfil que desempeña en el sistema.

3.8.2 Autorización

Una vez autenticados, definimos a qué recursos tiene permisos de acceso en nuestro sistema en base al role/perfil del usuario. Definimos en el descriptor de despliegue de nuestra aplicación (web.xml) estos roles, y a qué recursos tienen acceso:

```
<security-role>
        <role-name>user</role-name>
</security-role>
<security-role>
        <role-name>administrator</role-name>
</security-role>
<security-role>
        <role-name>solicitante</role-name>
</security-role>
<security-role>
        <role-name>tramitador</role-name>
</security-role>
<security-role>
        <role-name>responsable</role-name>
</security-role>

<security-constraint>
  <web-resource-collection>
  <web-resource-name>Acceso seguro ssl</web-resource-name>
<url-pattern>/*</url-pattern>
  </web-resource-collection>
  <user-data-constraint>
<transport-guarantee>CONFIDENTIAL</transport-guarantee>
  </user-data-constraint>
</security-constraint>

<security-constraint>
    <web-resource-collection>
        <web-resource-name>administrator pages</web-resource-name>
        <url-pattern>/administrador/*</url-pattern>
    </web-resource-collection>
    <auth-constraint>
        <role-name>administrator</role-name>
    </auth-constraint>
</security-constraint>

<security-constraint>
    <web-resource-collection>
        <web-resource-name>Solicitante pages</web-resource-name>
        <url-pattern>/solicitante/*</url-pattern>
    </web-resource-collection>
    <auth-constraint>
        <role-name>solicitante</role-name>
    </auth-constraint>
</security-constraint>
```

```
<security-constraint>
    <web-resource-collection>
        <web-resource-name>Tramitador pages</web-resource-name>
        <url-pattern>/tramitador/*</url-pattern>
    </web-resource-collection>
    <auth-constraint>
        <role-name>tramitador</role-name>
    </auth-constraint>
</security-constraint>

<security-constraint>
    <web-resource-collection>
        <web-resource-name>Responsable pages</web-resource-name>
        <url-pattern>/responsable/*</url-pattern>
    </web-resource-collection>
    <auth-constraint>
        <role-name>responsable</role-name>
    </auth-constraint>
</security-constraint>

<security-constraint>
    <web-resource-collection>
        <web-resource-name>Profile</web-resource-name>
        <url-pattern>/profile/*</url-pattern>
    </web-resource-collection>
    <auth-constraint>
        <role-name>administrator</role-name>
        <role-name>solicitante</role-name>
        <role-name>tramitador</role-name>
        <role-name>responsable</role-name>
    </auth-constraint>
</security-constraint>
```

3.8.3 Firma Electrónica

Como ya hemos descrito, usaremos la suite cliente @firma, en concreto la aplicación de escritorio Autofirma, que se integra con nuestra aplicación a través de la librería de javascript "autoscript.js" (última versión del obsoleto miniapplet.js) de la misma suite.
Esta librería dispone del método `sign`, al que le pasaremos un objeto json con la información de la solicitud a firmar (en formato base64) con el siguiente formato:

```
{
  "idFirma": "<UUID>",
  "idSistema": X,
  "idDerecho": Y
}
```

Se lanzará Autofirma que nos solicitará nuestro certificado personal con el que firmar, nos devolverá el control de manera asíncrona a una función de callback donde obtendremos: la firma en formato XMLDsig y el certificado utilizado. Estos datos se enviarán al componente ManagedBean JSF que tramita la petición del solicitante del derecho, donde se validará la firma (integridad y certificado en vigor del solicitante) antes de tramitar la solicitud, llamando a la operación `isValidSignature` del componente de negocio SeguridadBusiness. Para ello, usaremos la api estándar java de firma electrónica (`javax.xml.crypto.dsig.XMLSignature.validate`).

3.9 Decisiones de Diseño servicio web eRGPD

Se decide diseñar el servicio web que procesa las solicitudes síncronas, con una aproximación top-down dirigido por contrato, también llamado Contract-First. Es decir, diseñamos el descriptor del servicio web WSDL, y a partir de éste, generaremos los stubs cliente y servidor JAX-WS con la herramienta wsimport de la JDK.

El WSDL se puede consultar en el Anexo 2. Las decisiones reseñables en el diseño del web service son:

- En caso de error, devolveremos un *SOAPFault* del tipo definido *RGPDException*.
- En las operaciones de *acceso* y *portabilidad*, se devuelven los datos personales del tipo definido *InfomacionDatosPersonales*, al ser datos dependientes del sistema de información que está implementando el web service, se decide definirlo de tipo:

  ```
  <xsd:any minOccurs="0"/>
  ```

  Esta será la información que se devuelva al solicitante en un formato estructurado e interoperable como requiere el RGPD, XML. La implementación fake proporcionada devolverá siempre la misma información que recuperará de un fichero con datos de prueba (datosPersonalesFake.xml).
  El componente de la capa de negocio *SolicitudClientService* que hemos definido invocará al web service, y transformará estos datos personales obtenidos como objeto JAXB en un documento XML que se almacenará en la resolución asociada a la solicitud.

4. Construcción

4.1 Preparación del Entorno

Finalizada la fase de diseño, se definen los elementos necesarios para la generación del código del sistema de información eRGPD según la especificación del entorno tecnológico descrito en el apartado 3.6.
Para un mayor detalle, ver Anexo 1, con instrucciones de despliegue.

4.1.1 Implantación de Base de datos

Una vez instalado el gestor de base de datos postgreSQL y la utilidad de administración pgAdmin, se de alta un usuario (USER/PASSWORD). Se elabora y ejecuta el script proporcionado "init_bbdd.sql" para la creación del schema, tablas y carga inicial de datos necesario.

4.1.2 Implantación de servidor J2EE

Una vez instalado el servidor de aplicaciones Wildfly, se configura el driver jdbc de postgreSQL, DataSource, y almacenes de certificados (keystore y truststore) para el acceso seguro SSL.

4.1.3 Preparación Entorno de construcción

Para la construcción de la aplicación, se decide crear el proyecto desde maven, no solo por definir una estructura estándar, sino por las ventajas que nos proporciona en todo el ciclo de vida del proyecto, compilación, pruebas, despliegue. Como IDE, se decide usar "Eclipse IDE for Enterprise Java Developers (2019-12)".

4.2 Generación del código

Siguiendo el diseño definido, se desarrolla el código de los componentes de manera incremental y en paralelo a la ejecución de pruebas unitarias y de integración del sistema.

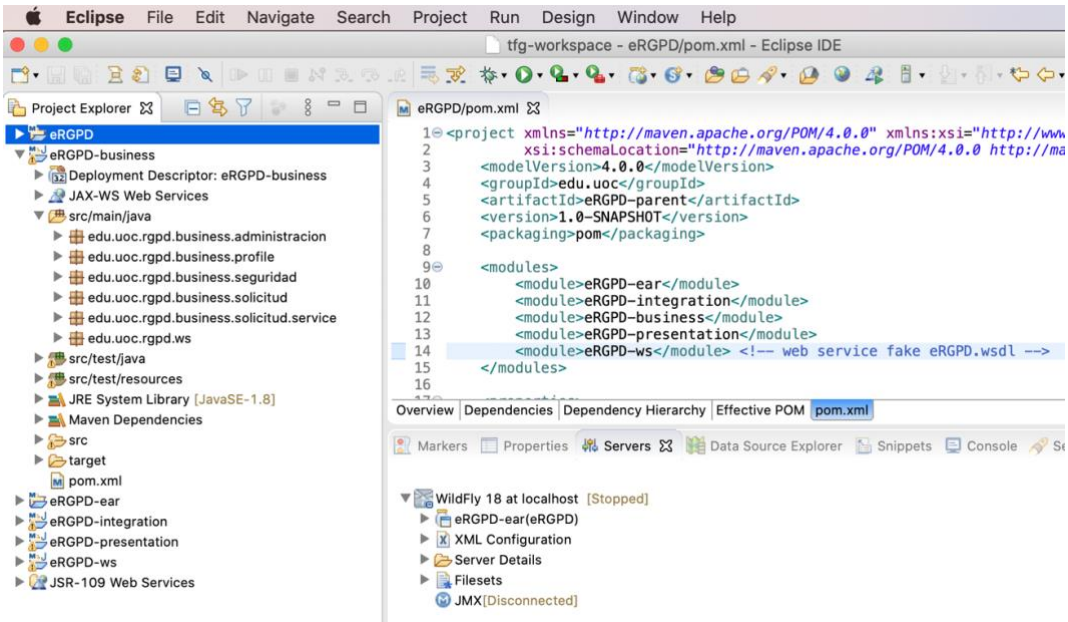


Figura 62. Proyecto eRGPD importado en Eclipse.

5. Pruebas

Con el fin de asegurar la calidad del producto y detectar posibles errores en las fases tempranas del desarrollo, se diseña un plan de pruebas con el objetivo de comprobar el correcto funcionamiento del sistema.

5.1 Diseño Pruebas

Verificamos el funcionamiento de todos los componentes de las capas de persistencia y negocio de manera automatizada en un entorno de ejecución real, verificando de esta manera que interactúan correctamente y que cumplen con la funcionalidad requerida. Estas pruebas unitarias y de integración, aunque es un proceso costoso, repercutirá de manera muy positiva en la realización de las pruebas funcionales que se realizarán de manera manual al no disponer del tiempo necesario para automatizarlas.

5.2 Automatización de las pruebas

Para automatizar las pruebas de todos los componentes de las capas de integración y negocio, usaremos maven, junit y el framework **Arquillian**.

5.2.1 Base de datos entorno de Integración

El script proporcionado para la construcción de los elementos de la base de datos del resto de entornos creará también un schema "rgpdtest" para la realización de las pruebas de integración. Las tablas se crearán automáticamente al desplegar los componentes de la capa de persistencia en el servidor wildfly del entorno de integración, que deberá de configurarse siguiendo las mismas instrucciones proporcionadas (o ser la misma instancia) para configurar el servidor del entorno de desarrollo.

5.2.1.1 Datos de prueba

Los datos de pruebas se cargan automáticamente al ejecutar las pruebas. Tanto en los sub-módulos de la capa de integración como de negocio, en la carpeta "src/test/resources/scripts" encontraremos un archivo "populate-data.sql", así como en la carpeta "src/test/resources/datasets" tendremos un fichero xml con los datos esperados para cada uno de los métodos de test de los componentes que modifican la base de datos.

También, se proporciona en la carpeta "src/test/resources/firmas", un fichero "firma.xsig" (una solicitud firmada de un derecho) y mi certificado personal "cesar.cer" (parte pública) para las pruebas del componente de seguridad encargado del login con certificado y la validación de las firmas XMLDsig de las solicitudes presentadas.

5.2.2 Servidor J2EE de Integración

Usaremos el mismo servidor wildfly configurado en la fase de construcción del sistema. No existe conflicto entre la ejecución de las pruebas y el despliegue de la aplicación en el mismo servidor.

5.3 Ejecución de las pruebas de Integración

Levantamos el servidor wildfly del entorno de integración (en nuestro caso el mismo que el de desarrollo y en la misma máquina) en un terminal. Si se ejecuta en un puerto distinto al de una instalación por defecto (puerto de administración 9090) y usuario (USER/PASSWORD), habría que configurar el fichero de configuración "arquillian.xml" con los datos de acceso al servidor wildfly:

```
<container qualifier="widlfly-remote">
    <configuration>
        <property name="managementAddress">127.0.0.1</property>
        <property name="managementPort">9990</property>
        <property name="username">USER</property>
        <property name="password">PASSWORD</property>
    </configuration>
</container>
```

A continuación, abrimos otro terminal y desde el directorio raíz del proyecto "eRGPD" (donde se encuentra el pom.xml padre), ejecutamos:

```
mvn clean test -Parq-wildfly-remote
```

La ejecución de las pruebas de integración pueden tardar varios minutos. Al terminar, se mostrará que se han pasado correctamente.

```
[INFO] ------------------------------------------------------------------------
[INFO] Reactor Summary for eRGPD-parent 1.0-SNAPSHOT:
[INFO]
[INFO] eRGPD-parent ....................................... SUCCESS [  0.099 s]
[INFO] eRGPD-integration .................................. SUCCESS [02:20 min]
[INFO] eRGPD-business ..................................... SUCCESS [02:26 min]
[INFO] eRGPD-presentation ................................. SUCCESS [  0.353 s]
[INFO] eRGPD-ws ........................................... SUCCESS [  0.155 s]
[INFO] eRGPD-ear .......................................... SUCCESS [  0.242 s]
[INFO] ------------------------------------------------------------------------
[INFO] BUILD SUCCESS
[INFO] ------------------------------------------------------------------------
[INFO] Total time:  04:48 min
[INFO] Finished at: 2020-05-19T23:06:16+02:00
[INFO] ------------------------------------------------------------------------
```

Figura 63. Ejecución correcta pruebas unitarias y de integración

Maven, generará en la carpeta "target/surefire-reports", el detalle del resultado de las pruebas de cada componente en formato xml y txt.

```
▼<testsuite name="edu.uoc.rgpd.business.seguridad.SeguridadFacadeTest" time="15.844" tests="4" errors="0" skipped="0" failures="0">
  ▶<properties>...</properties>
   <testcase name="loginCertificateTest" classname="edu.uoc.rgpd.business.seguridad.SeguridadFacadeTest" time="4.085"/>
   <testcase name="loginTest" classname="edu.uoc.rgpd.business.seguridad.SeguridadFacadeTest" time="3.915"/>
   <testcase name="isValidSignatureTest" classname="edu.uoc.rgpd.business.seguridad.SeguridadFacadeTest" time="3.945"/>
   <testcase name="getX509CertificateTest" classname="edu.uoc.rgpd.business.seguridad.SeguridadFacadeTest" time="3.899"/>
 </testsuite>
```

Figura 64. Ejecución pruebas del componente de negocio SeguridadFacade.

```
▼<testsuite name="edu.uoc.rgpd.business.solicitud.SolicitudFacadeTest" time="47.467" tests="12" errors="0" skipped="0" failures="0">
  ▶<properties>...</properties>
   <testcase name="findAllDerechosTest" classname="edu.uoc.rgpd.business.solicitud.SolicitudFacadeTest" time="4.398"/>
   <testcase name="tramitarSolicitudAsincronaTest" classname="edu.uoc.rgpd.business.solicitud.SolicitudFacadeTest" time="3.919"/>
   <testcase name="totalByEstadoTest" classname="edu.uoc.rgpd.business.solicitud.SolicitudFacadeTest" time="3.903"/>
   <testcase name="getSolicitudTest" classname="edu.uoc.rgpd.business.solicitud.SolicitudFacadeTest" time="3.947"/>
   <testcase name="findBySistemaEstadoTest" classname="edu.uoc.rgpd.business.solicitud.SolicitudFacadeTest" time="3.921"/>
   <testcase name="getDocumentoTest" classname="edu.uoc.rgpd.business.solicitud.SolicitudFacadeTest" time="3.919"/>
   <testcase name="findByTramitadorEstadoTest" classname="edu.uoc.rgpd.business.solicitud.SolicitudFacadeTest" time="3.911"/>
   <testcase name="totalBySistemaEstadoTest" classname="edu.uoc.rgpd.business.solicitud.SolicitudFacadeTest" time="3.902"/>
   <testcase name="addSolicitudTest" classname="edu.uoc.rgpd.business.solicitud.SolicitudFacadeTest" time="3.906"/>
   <testcase name="findBySolicitanteTest" classname="edu.uoc.rgpd.business.solicitud.SolicitudFacadeTest" time="3.898"/>
   <testcase name="totalByTramitadorEstadoTest" classname="edu.uoc.rgpd.business.solicitud.SolicitudFacadeTest" time="3.907"/>
   <testcase name="findBySistemaDerechoEstadoTest" classname="edu.uoc.rgpd.business.solicitud.SolicitudFacadeTest" time="3.936"/>
 </testsuite>
```

Figura 65. Ejecución pruebas del componente de negocio SolicitudFacade.

6. Conclusiones

El primer aspecto que me gustaría destacar en estas conclusiones es la dificultad de encontrar un proyecto interesante, que resolviera un problema real que resultara de gran utilidad. Un trabajo fin de grado que aportara valor añadido y que se pudiera abordar en este contexto, en otras palabras, esa idea original inicial: ¿qué hacer?

En cuanto al desarrollo del proyecto, he logrado los objetivos siguiendo la planificación y metodología planteada. No obstante, no ha sido un camino fácil, y tengo que reconocer que fui demasiado ambicioso en los objetivos a alcanzar, con toda seguridad por un exceso de confianza basada en mi experiencia laboral en desarrollos J2EE y haber planificado mis estudios de grado para que en este último semestre solo tuviera que centrarme en este TFG, por todo lo cual, no medí adecuadamente el esfuerzo de elaborar una documentación detallada para la realización del análisis y diseño de la aplicación, lo que a la postre provocó un sobreesfuerzo para poder entregar en plazo.

Decidí ceñirme a la especificación J2EE para el diseño del sistema y no incorporar dependencias de terceros en la medida de lo posible, por su repercusión en la portabilidad del sistema, y salvar posibles restricciones que las organizaciones que pudieran implantar nuestro sistema pudieran definir. Además, a título personal, quería enfrentarme a un proyecto J2EE sin usar frameworks a los que habitualmente recurro en mi entorno laboral, y comprobar si está justificado el uso de éstos frente a este enfoque "austero" por el que he optado, con el fin también de medir la supuesta distancia que separa ambos planteamientos para proyectos que afronte en el futuro. Y las conclusiones a las que he llegado basándome en esta experiencia son:

- JPA. Un acierto, volvería a utilizarlo, en este aspecto la distancia que pudo existir en el pasado entre cualquier ORM y el acceso directo con JDBC (o peor aún, los antiguos EJB's de entidad) está resuelta. Hibernate es la implementación JPA por defecto y no se justifica el uso de una librería propietaria, ya sea ésta (accediendo desde sus propias clases en vez de a través de la api) u otra.
- EJB's. Al igual que en el caso anterior, en la capa de negocio, siempre que necesitara diseñar una arquitectura orientada a componentes distribuidos, volvería a utilizarlos. No he echado en falta un framework como spring en este caso, dado que la especificación, aporta características como la inversión del control y la inyección de dependencias de igual manera.
- JSF. En la capa de presentación, si que he tenido más dificultades y creo que la brecha entre esta especificación estándar J2EE y las alternativas disponibles en el mercado es más acentuada que en los casos anteriores. Y no creo que me decante por volver a usarlo en el futuro.
- Java EE Security API. Es posible que en algún proyecto con requisitos de seguridad más laxos decidiera usarlo de nuevo. Pero la adaptabilidad que proporciona spring security en un escenario como el del proyecto abordado justificaría su uso y lo he echado de menos.

Centrándome ahora en la fase de construcción del sistema, como en cualquier otro proyecto pero que se pone de manifiesto de manera más acentuada en uno que se aborda en solitario, cabe destacar que es difícil en distintos momentos no darse de bruces con algún problema técnico no contemplado o algún caso de uso al que no diera la suficiente

importancia en la planificación a la hora de definir su alcance. Entre éstos, destacaría los siguientes:

- Configuración SSL del servidor wildfly.
- Integración con Autofirma.
- Pruebas de Integración con framework Arquillian.
- Curva aprendizaje de Java Server Faces.

Como líneas del trabajo para el futuro no abordadas en este TFG, señalaría:

- Plataforma de comunicaciones. Notificar al solicitante de cambios de estado en sus solicitudes.
- Firma electrónica de las resoluciones con certificado de servidor.
- Visor de documentos firmados.
- Firma longeva, integración con alguna plataforma de firma. Uso de formato XADES-T, añadir sello de tiempo a la firma para garantizar la validez de la firma una vez el certificado haya caducado.
- Integración real con sistema de información que trate datos de carácter personal.
- Integración Continua. Con el objetivo de evolucionar el sistema de manera ágil y con parámetros de calidad definidos.

En algunos casos, no se han llevado a cabo no ya por su complejidad técnica, que en mayoría de los casos no suponía mayor complicación, como es el caso del envío de emails para notificar un cambio de estado en las solicitudes, sino por motivos de tiempo disponible.

Para concluir, estoy satisfecho con el trabajo realizado, me ha dado la oportunidad de salir de mi zona de confort, y he descubierto herramientas muy útiles como Lucidchart y Balsamiq wireframes que desconocía.

7. Glosario

RGPD: Reglamento General de Protección de Datos

Interesado: Persona física titular de los datos que sean objeto del tratamiento.

Datos Personales: toda información sobre una persona física identificada o identificable («el interesado»)

Tratamiento: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no

Responsable del tratamiento: Cualquier organización, persona o entidad que determine los propósitos y medios para el tratamiento de datos personales, controle los datos y sea responsable de ello, solo o conjuntamente

Encargado del tratamiento: El encargado del tratamiento es la persona física o jurídica, autoridad, servicio u otro organismo que presta un servicio al responsable que conlleva el tratamiento de datos personales por cuenta de éste.

Consentimiento: Toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen.

AEPD: Agencia Española de Protección de Datos.

FNMT: Fábrica Nacional de Moneda y Timbre.

XMLDsig: Síntaxis XML para la firma digital.

autofirm@: Aplicación de escritorio de firma electrónica.

Arquillian: framework que permite deshacernos de los mocks y escribir pruebas reales. Se ejecutan en el propio contenedor J2EE.

8. Bibliografía

- BOE. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. [Consulta: 02/2020] <https://boe.es/buscar/act.php?id=BOE-A-2018-16673>

- Agencia Española de Protección de Datos. [Consulta: 02/2020] <https://www.aepd.es/es/derechos-y-deberes/conoce-tus-derechos>

- WildFly Elytron Security. [Consulta: 04/2020] <https://docs.wildfly.org/18/WildFly_Elytron_Security.html#configure-ssltls>

- Firma electrónica. [Consulta: 05/2020] <https://firmaelectronica.gob.es/>

- Cliente de firma electrónica de @firma. [Consulta: 05/2020] <https://administracionelectronica.gob.es/ctt/clienteafirma>

- XML Digital Signature API. [Consulta: 05/2020] <https://docs.oracle.com/javase/8/docs/technotes/guides/security/xmldsig/XMLDigitalSignature.html>

- Valide. [Consulta: 05/2020] <https://valide.redsara.es/valide/ejecutarValidarFirma/ejecutar.html>

- Arquillian. [Consulta: 04/2020] <http://arquillian.org/>

- Arquillian Persistence Extension. [Consulta: 04/2020] <http://arquillian.org/arquillian-extension-persistence/>

9. Anexo 1. Implantación

9.1 Requisitos de Implantación

Describimos los requisitos de implantación del sistema eRGPD. Con el objetivo de facilitar la puesta en marcha de la aplicación, se proporcionan ficheros de configuración para sobre escribir los originales de una instalación limpia del servidor wildfly. También se proporcionan el certificado ssl del servidor (autofirmado) almacenado en "server.keystore" y un almacén de certificados de confianza "client.truststore" que contiene el certificado raíz de la CA de la FNMT.

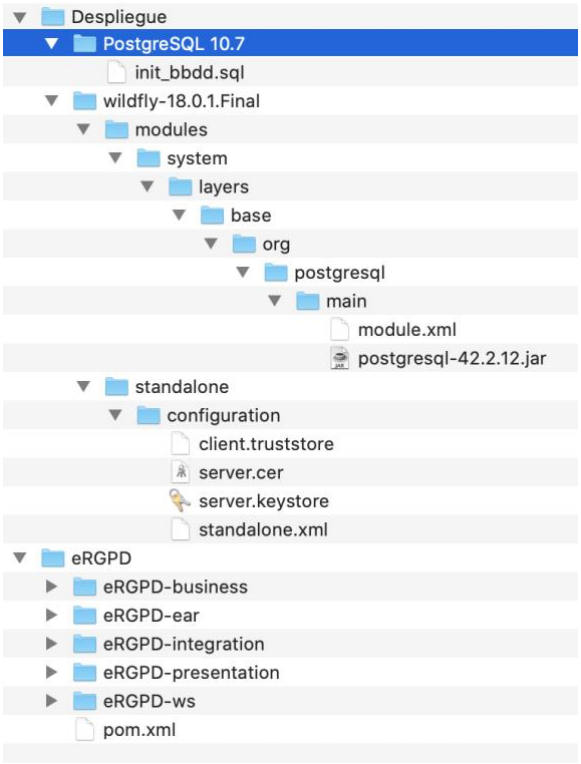


Figura 66. Estructura entregable

Carpetas:
/eRGPD: Código fuente (maven multimódulo):
- /eRGPD-business: capa de negocio (jar)
- /eRGPD-ear: construcción ear
- /eRGPD-integration: capa de persistencia (jar)
- /eRGPD-presention: capa de presentación (war)
- /eRGPD-ws: webservice implementación fake (jar)

/Despliegue: Ficheros de configuración
- /PostgreSQL 10.7: script "init_bbdd.sql"
- /wildfly-18.0.1.Final: configuración, keystore, trustore y driver.
  - …/standalone.xml
  - …/client.truststore
  - …/server.keystore: almacena par key/certificado ssl (server.cer).
  - …/server.cer (certificado de servidor a importar como certificado de confianza en navegador)

…/module.xml
…/postgresql-42.2.12.jar (driver jbdc)

9.1.1 PostgreSQL 10.7

Daremos de alta un usuario con permisos de lectura y escritura a la base de datos desde la consola de administración. Serán necesarios para dar de alta el datasource en el servidor wildfly. Los ficheros de configuración aportados están configurados con los siguientes datos:

Usuario: USER
Password: PASSWORD
BBDD: postgres (creada por defecto)

A continuación, se ejecuta script (desde pg Admin 4) suministrado: "init_bbdd.sql" para crear el schema y las tablas, así como los datos iniciales necesarios (derechos del RGPD). Adicionalmente, para facilitar las pruebas, se dan de alta 2 sistemas de información (NOMINAS y RRHH), responsables del tratamiento y tramitadores, si bien, el propio sistema permite realizar estas tareas al usuario con perfil administrador.

9.1.2 Wildfly-18.0.1.Final

Una vez instalado, debemos configurar el acceso a través de SSL (keystore y truststore), datasource y driver jdbc en el fichero de configuración "standalone.xml". Se proporciona dicho fichero ya configurado, no obstante, se describen los elementos del fichero que han sido objeto de modificación en los siguientes apartados:

SSL

Es necesario habilitar el acceso seguro SSL, configuramos:

- Un keystore (server.keystore) donde almacenar el certificado del servidor wildfly (server.cer). Este certificado SSL, hay que importarlo como certificado de confianza del navegador web con el que accedemos a la aplicación.
- Un truststore, almacén de certificados de confianza (client.truststore) donde almacenar el certificado Raíz de la FNMT para poder acceder con nuestro certificado personal (necesario para poder firmar con Autofirma).

Configuración tls

```
<tls>
    <key-stores>
        <key-store name="twoWayKS">
            <credential-reference clear-text="secret"/>
            <implementation type="JKS"/>
            <file path="server.keystore" relative-to="jboss.server.config.dir"/>
        </key-store>
        <key-store name="twoWayTS">
            <credential-reference clear-text="secret"/>
            <implementation type="JKS"/>
            <file path="client.truststore" relative-to="jboss.server.config.dir"/>
        </key-store>
    </key-stores>
    <key-managers>
        <key-manager name="twoWayKM" key-store="twoWayKS">
            <credential-reference clear-text="secret"/>
        </key-manager>
    </key-managers>
    <trust-managers>
        <trust-manager name="twoWayTM" key-store="twoWayTS"/>
    </trust-managers>
    <server-ssl-contexts>
        <server-ssl-context name="twoWaySSC" protocols="TLSv1.2" need-client-auth="true" key-manager="twoWayKM" trust-manager="twoWayTM"/>
    </server-ssl-contexts>
</tls>
```

Configuración https

```
<subsystem xmlns="urn:jboss:domain:undertow:10.0" default-server="default-server" default-virtual-host="default-host" default-servlet-container="default" default-security-domain="other" statistics-enabled="${wildfly.undertow.statistics-enabled:${wildfly.statistics-enabled:false}}">
    <buffer-cache name="default"/>
    <server name="default-server">
        <http-listener name="default" socket-binding="http" redirect-socket="https" enable-http2="true"/>
        <https-listener name="https" socket-binding="https" ssl-context="twoWaySSC" enable-http2="true"/>
        <host name="default-host" alias="localhost">
            <location name="/" handler="welcome-content"/>
            <http-invoker security-realm="ApplicationRealm"/>
        </host>
    </server>
    <servlet-container name="default" default-encoding="UTF-8" use-listener-encoding="true">
        <jsp-config/>
        <websockets/>
    </servlet-container>
    <handlers>
        <file name="welcome-content" path="${jboss.home.dir}/welcome-content"/>
    </handlers>
</subsystem>
```

DataSource y driver jdbc postgresql-42.2.12.jar

Configuración Datasource

Configurar host y puerto del servidor postgres donde resida la BBDD.

```
<datasource jta="false" jndi-name="java:jboss/postgresDS" pool-name="postgresDS" enabled="true" use-java-context="true" use-ccm="false">
    <connection-url>jdbc:postgresql://localhost:5432/postgres</connection-url>
    <driver-class>org.postgresql.Driver</driver-class>
    <driver>postgresql</driver>
    <security>
        <user-name>USER</user-name>
        <password>PASSWORD</password>
    </security>
</datasource>
```

Configuración driver postgreSQL

```
<driver name="postgresql" module="org.postgresql">
    <driver-class>org.postgresql.Driver</driver-class>
    <xa-datasource-class>org.postgresql.xa.PGXADataSource</xa-datasource-class>
</driver>
```

9.1.3 Google Chrome (o cualquier navegador)

Importar como certificado de confianza el certificado del servidor suministrado “server.cer”
Importar su certificado personal de la FNMT.
Dependiendo del navegador y del sistema operativo, los certificados almacenarán en un sitio u otro. En el caso de Chrome/MacOS, se importan en un almacén del propio sistema operativo:

Figura 67. Almacén certificados

9.1.4 Autofirma 1.6.5

El cliente de @firma se libera como software libre de fuentes abiertas con una licencia: GNU GPL versión 2 y EUPL v1.1. Y nos podemos descargar la aplicación autofirma de la siguiente url:
https://administracionelectronica.gob.es/ctt/clienteafirma

9.2 Construcción y Despliegue

9.2.1 Construcción

Definimos una variable de entorno "MAVEN_HOME", y añadimos al PATH una ruta a "MAVEN_HOME/bin" para que encuentre el comando mvn.
Desde un terminal, ejecutamos desde la carpeta "eRGPD":

```
mvn clean install
```

```
[INFO] Installing /Users/cesar/tfg-workspace/eRGPD/eRGPD-ear/pom.xml to /Users/c
esar/.m2/repository/edu/uoc/eRGPD-ear/1.0-SNAPSHOT/eRGPD-ear-1.0-SNAPSHOT.pom
[INFO] ------------------------------------------------------------------------
[INFO] Reactor Summary for eRGPD-parent 1.0-SNAPSHOT:
[INFO]
[INFO] eRGPD-parent ....................................... SUCCESS [  0.223 s]
[INFO] eRGPD-integration .................................. SUCCESS [  1.905 s]
[INFO] eRGPD-business ..................................... SUCCESS [  0.461 s]
[INFO] eRGPD-presentation ................................. SUCCESS [  1.243 s]
[INFO] eRGPD-ws ........................................... SUCCESS [  0.190 s]
[INFO] eRGPD-ear .......................................... SUCCESS [  1.100 s]
[INFO] ------------------------------------------------------------------------
[INFO] BUILD SUCCESS
[INFO] ------------------------------------------------------------------------
[INFO] Total time:  5.278 s
[INFO] Finished at: 2020-05-15T08:08:03+02:00
[INFO] ------------------------------------------------------------------------
Cesars-MacBook-Pro:eRGPD cesar$
```

Figura 68. Salida terminal: "mvn clean install"

Nos genera los artefactos en las carpetas target.

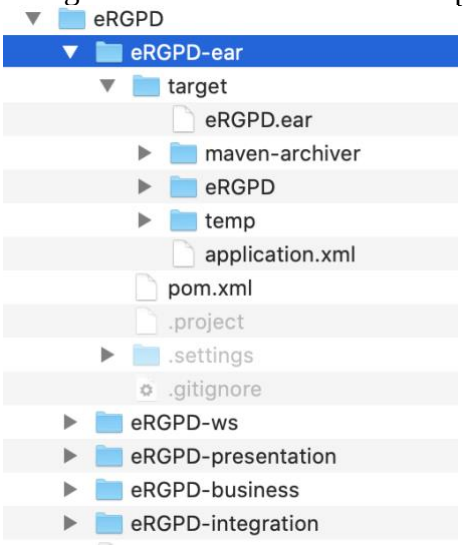


Figura 69. Artefactos generados

9.2.2 Despliegue

Con el servidor wildfly levantado con la configuración por defecto (puerto 8080) y habiendo dado de alta un usuario (USER/PASSWORD) con el comando "add-user", y definido una variable de entorno JBOSS_HOME con la ruta al directorio de instalación del servidor, podemos desplegar "eRGPD.ear" con maven.

Ejecutamos desde la carpeta "/eRGPD/eRGPD-ear"

```
mvn wildfly:deploy
```

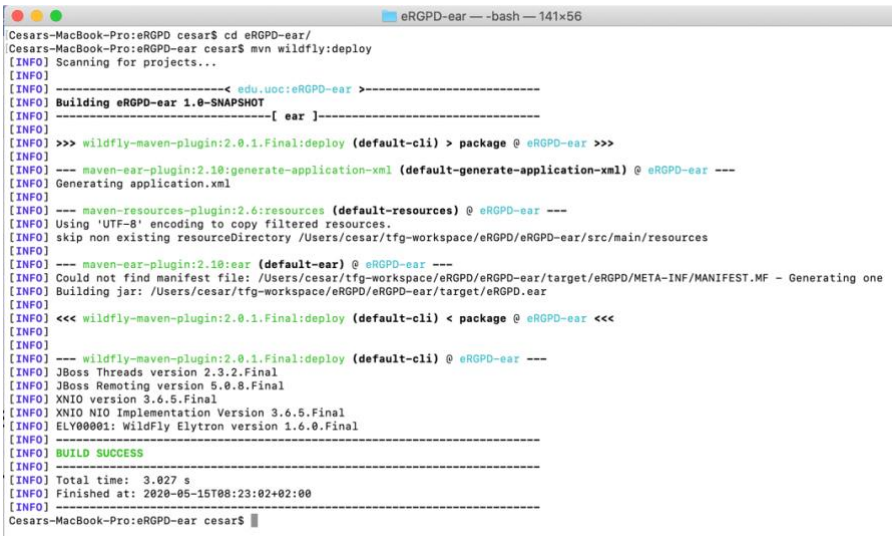


Figura 70. Salida terminal: "mvn wildfly:deploy"

9.2.2.1 Diagrama de despliegue

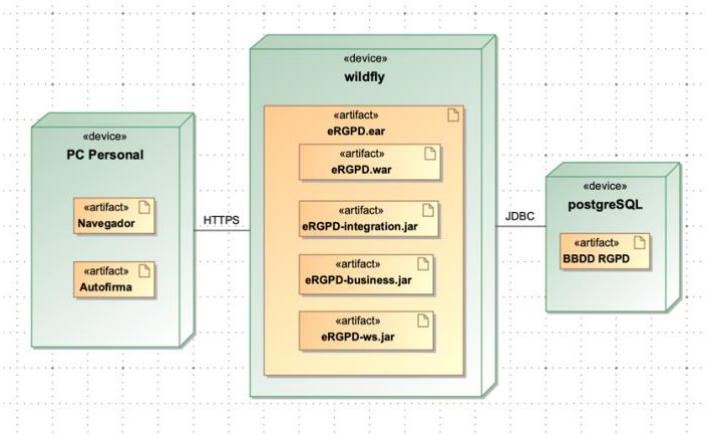


Figura 71. Diagrama de despliegue

No obstante, hay que tener en cuenta que en un entorno de producción, el artefacto eRGPD-ws (implementación dummy del interfaz wsdl), tendría tantas instancias desplegadas (implementaciones reales) como sistemas de información demos de alta en eRGPD que gestionen datos de carácter personal en la organización con el fin de poder tramitar las solicitudes de los interesados de manera síncrona.

9.2.3 Comprobación

Accedemos desde el navegador a la url "https://localhost:8443/eRGPD/" (localhost o el nombre del host y puerto donde hayamos desplegado).
Nos pedirá que seleccionemos nuestro certificado personal:

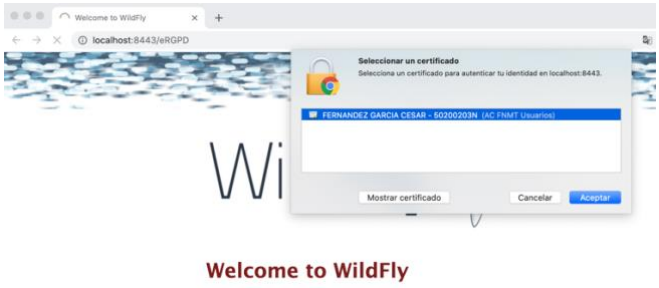


Figura 72. https. Selección de certificado

Y accederemos a la aplicación, donde podremos logarnos con el certificado presentado o con usuario/password (funcionalidad implementada para facilitar las pruebas).

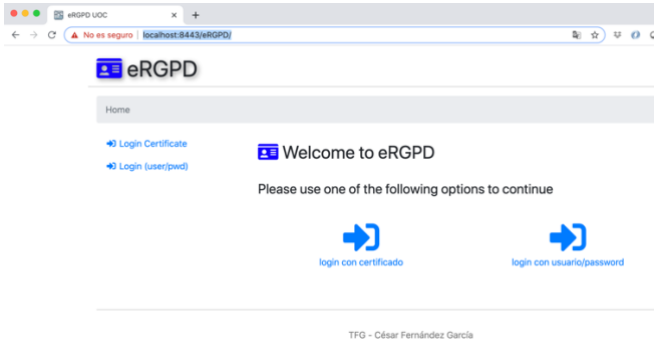


Figura 73. Pantalla de acceso a eRGPD

10. Anexo 2. Web Service eRGPD.

Descripción del servicio web eRGPD que implementarán los sistemas de información de la organización para un tratamiento síncrono de las solicitudes presentadas a dicho sistema.

10.1 Descriptor WSDL

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<wsdl:definitions xmlns:rgpd="http://www.tfg.uoc.edu/eRGPD/"
xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/" xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema" name="eRGPD"
targetNamespace="http://www.tfg.uoc.edu/eRGPD/">
  <wsdl:types>
    <schema xmlns="http://www.w3.org/2001/XMLSchema">
      <import namespace="http://www.tfg.uoc.edu/eRGPD/" schemaLocation="eRGPD.xsd" />
    </schema>
  </wsdl:types>
  <wsdl:message name="RGPDException">
    <wsdl:part name="fault" element="rgpd:RGPDError"/>
  </wsdl:message>
  <wsdl:message name="AccesoRequest">
    <wsdl:part element="rgpd:Acceso" name="parameters"/>
  </wsdl:message>
  <wsdl:message name="AccesoResponse">
    <wsdl:part element="rgpd:AccesoResponse" name="parameters"/>
  </wsdl:message>
  <wsdl:message name="RectificacionRequest">
    <wsdl:part element="rgpd:Rectificacion" name="parameters"/>
  </wsdl:message>
  <wsdl:message name="RectificacionResponse">
    <wsdl:part element="rgpd:RectificacionResponse" name="parameters"/>
  </wsdl:message>
  <wsdl:message name="OposicionRequest">
    <wsdl:part element="rgpd:Oposicion" name="parameters"/>
  </wsdl:message>
  <wsdl:message name="OposicionResponse">
```

```
  <wsdl:part element="rgpd:OposicionResponse" name="parameters"/>
</wsdl:message>
<wsdl:message name="SupresionRequest">
  <wsdl:part element="rgpd:Supresion" name="parameters"/>
</wsdl:message>
<wsdl:message name="SupresionResponse">
  <wsdl:part element="rgpd:SupresionResponse" name="parameters"/>
</wsdl:message>
<wsdl:message name="LimitacionRequest">
  <wsdl:part element="rgpd:Limitacion" name="parameters"/>
</wsdl:message>
<wsdl:message name="LimitacionResponse">
  <wsdl:part element="rgpd:LimitacionResponse" name="parameters"/>
</wsdl:message>
<wsdl:message name="PortabilidadRequest">
  <wsdl:part element="rgpd:Portabilidad" name="parameters"/>
</wsdl:message>
<wsdl:message name="PortabilidadResponse">
  <wsdl:part element="rgpd:PortabilidadResponse" name="parameters"/>
</wsdl:message>
<wsdl:message name="DecisionesAutomatizadasRequest">
  <wsdl:part element="rgpd:DecisionesAutomatizadas" name="parameters"/>
</wsdl:message>
<wsdl:message name="DecisionesAutomatizadasResponse">
  <wsdl:part element="rgpd:DecisionesAutomatizadasResponse" name="parameters"/>
</wsdl:message>

<wsdl:portType name="eRGPD">
  <wsdl:operation name="Acceso">
    <wsdl:input message="rgpd:AccesoRequest"/>
    <wsdl:output message="rgpd:AccesoResponse"/>
    <wsdl:fault message="rgpd:RGPDException" name="RGPDException"/>
  </wsdl:operation>
  <wsdl:operation name="Rectificacion">
    <wsdl:input message="rgpd:RectificacionRequest"/>
    <wsdl:output message="rgpd:RectificacionResponse"/>
    <wsdl:fault message="rgpd:RGPDException" name="RGPDException"/>
  </wsdl:operation>
  <wsdl:operation name="Supresion">
    <wsdl:input message="rgpd:SupresionRequest"/>
    <wsdl:output message="rgpd:SupresionResponse"/>
    <wsdl:fault message="rgpd:RGPDException" name="RGPDException"/>
  </wsdl:operation>
  <wsdl:operation name="Oposicion">
    <wsdl:input message="rgpd:OposicionRequest"/>
    <wsdl:output message="rgpd:OposicionResponse"/>
    <wsdl:fault message="rgpd:RGPDException" name="RGPDException"/>
  </wsdl:operation>
  <wsdl:operation name="Limitacion">
    <wsdl:input message="rgpd:LimitacionRequest"/>
    <wsdl:output message="rgpd:LimitacionResponse"/>
    <wsdl:fault message="rgpd:RGPDException" name="RGPDException"/>
  </wsdl:operation>
  <wsdl:operation name="Portabilidad">
    <wsdl:input message="rgpd:PortabilidadRequest"/>
    <wsdl:output message="rgpd:PortabilidadResponse"/>
    <wsdl:fault message="rgpd:RGPDException" name="RGPDException"/>
  </wsdl:operation>
  <wsdl:operation name="DecisionesAutomatizadas">
    <wsdl:input message="rgpd:DecisionesAutomatizadasRequest"/>
    <wsdl:output message="rgpd:DecisionesAutomatizadasResponse"/>
    <wsdl:fault message="rgpd:RGPDException" name="RGPDException"/>
  </wsdl:operation>
</wsdl:portType>
<wsdl:binding name="eRGPDSOAP" type="rgpd:eRGPD">
  <soap:binding style="document" transport="http://schemas.xmlsoap.org/soap/http"/>
  <wsdl:operation name="Acceso">
    <soap:operation soapAction="http://www.tfg.uoc.edu/eRGPD/Acceso"/>
    <wsdl:input>
      <soap:body use="literal"/>
    </wsdl:input>
    <wsdl:output>
      <soap:body use="literal"/>
    </wsdl:output>
    <wsdl:fault name="RGPDException">
      <soap:fault name="RGPDException" use="literal"/>
    </wsdl:fault>
  </wsdl:operation>
  <wsdl:operation name="Rectificacion">
```

```
      <soap:operation soapAction="http://www.tfg.uoc.edu/eRGPD/Rectificacion"/>
      <wsdl:input>
        <soap:body use="literal"/>
      </wsdl:input>
      <wsdl:output>
        <soap:body use="literal"/>
      </wsdl:output>
      <wsdl:fault name="RGPDException">
        <soap:fault name="RGPDException" use="literal"/>
      </wsdl:fault>
    </wsdl:operation>
    <wsdl:operation name="Supresion">
      <soap:operation soapAction="http://www.tfg.uoc.edu/eRGPD/Supresion"/>
      <wsdl:input>
        <soap:body use="literal"/>
      </wsdl:input>
      <wsdl:output>
        <soap:body use="literal"/>
      </wsdl:output>
      <wsdl:fault name="RGPDException">
        <soap:fault name="RGPDException" use="literal"/>
      </wsdl:fault>
    </wsdl:operation>
    <wsdl:operation name="Oposicion">
      <soap:operation soapAction="http://www.tfg.uoc.edu/eRGPD/Oposicion"/>
      <wsdl:input>
        <soap:body use="literal"/>
      </wsdl:input>
      <wsdl:output>
        <soap:body use="literal"/>
      </wsdl:output>
      <wsdl:fault name="RGPDException">
        <soap:fault name="RGPDException" use="literal"/>
      </wsdl:fault>
    </wsdl:operation>
    <wsdl:operation name="Limitacion">
      <soap:operation soapAction="http://www.tfg.uoc.edu/eRGPD/Limitacion"/>
      <wsdl:input>
        <soap:body use="literal"/>
      </wsdl:input>
      <wsdl:output>
        <soap:body use="literal"/>
      </wsdl:output>
      <wsdl:fault name="RGPDException">
        <soap:fault name="RGPDException" use="literal"/>
      </wsdl:fault>
    </wsdl:operation>
    <wsdl:operation name="Portabilidad">
      <soap:operation soapAction="http://www.tfg.uoc.edu/eRGPD/Portabilidad"/>
      <wsdl:input>
        <soap:body use="literal"/>
      </wsdl:input>
      <wsdl:output>
        <soap:body use="literal"/>
      </wsdl:output>
      <wsdl:fault name="RGPDException">
        <soap:fault name="RGPDException" use="literal"/>
      </wsdl:fault>
    </wsdl:operation>
    <wsdl:operation name="DecisionesAutomatizadas">
      <soap:operation soapAction="http://www.tfg.uoc.edu/eRGPD/DecisionesAutomatizadas"/>
      <wsdl:input>
        <soap:body use="literal"/>
      </wsdl:input>
      <wsdl:output>
        <soap:body use="literal"/>
      </wsdl:output>
      <wsdl:fault name="RGPDException">
        <soap:fault name="RGPDException" use="literal"/>
      </wsdl:fault>
    </wsdl:operation>
  </wsdl:binding>
  <wsdl:service name="eRGPD">
    <wsdl:port binding="rgpd:eRGPDSOAP" name="eRGPDSOAP">
      <soap:address location="http://<hostname>:<port>/eRGPD-ws-1.0-SNAPSHOT/eRGPD?wsdl"/>
    </wsdl:port>
  </wsdl:service>
</wsdl:definitions>
```

10.2 Schema

```
<?xml version="1.0" encoding="UTF-8"?>
<xsd:schema xmlns="http://www.tfg.uoc.edu/eRGPD/"
        xmlns:xsd="http://www.w3.org/2001/XMLSchema"
        targetNamespace="http://www.tfg.uoc.edu/eRGPD/"
        elementFormDefault="qualified">

      <xsd:element name="RGPDError" type="RGPDError" nillable="true"/>
      <xsd:element name="Acceso" type="Acceso"/>
      <xsd:element name="AccesoResponse" type="AccesoResponse"/>
      <xsd:element name="Rectificacion" type="Rectificacion"/>
      <xsd:element name="RectificacionResponse" type="RectificacionResponse"/>
      <xsd:element name="Oposicion" type="Oposicion"/>
      <xsd:element name="OposicionResponse" type="OposicionResponse"/>
      <xsd:element name="Supresion" type="Supresion"/>
      <xsd:element name="SupresionResponse" type="SupresionResponse"/>
      <xsd:element name="Limitacion" type="Limitacion"/>
      <xsd:element name="LimitacionResponse" type="LimitacionResponse"/>
      <xsd:element name="Portabilidad" type="Portabilidad"/>
      <xsd:element name="PortabilidadResponse" type="PortabilidadResponse"/>
      <xsd:element name="DecisionesAutomatizadas" type="DecisionesAutomatizadas"/>
      <xsd:element name="DecisionesAutomatizadasResponse" type="DecisionesAutomatizadasResponse"/>
      <xsd:complexType name="RGPDError">
        <xsd:sequence>
          <xsd:element name="Mensaje" type="xsd:string"/>
        </xsd:sequence>
      </xsd:complexType>
      <xsd:complexType name="Acceso">
        <xsd:sequence>
          <xsd:element name="Solicitante" type="xsd:string"/>
        </xsd:sequence>
      </xsd:complexType>
      <xsd:complexType name="AccesoResponse">
        <xsd:sequence>
          <xsd:element name="Resultado" type="Resultado" minOccurs="0"/>
        </xsd:sequence>
      </xsd:complexType>
      <xsd:complexType name="Rectificacion">
        <xsd:sequence>
            <xsd:element name="Solicitante" type="xsd:string"/>
            <xsd:element name="DatosIntorrectos" type="xsd:string"/>
            <xsd:element name="DocumentacionAcreditacion" type="xsd:base64Binary" />
        </xsd:sequence>
      </xsd:complexType>
      <xsd:complexType name="RectificacionResponse">
        <xsd:sequence>
          <xsd:element name="Resultado" type="Resultado" minOccurs="0"/>
        </xsd:sequence>
      </xsd:complexType>
      <xsd:complexType name="Oposicion">
        <xsd:sequence>
            <xsd:element name="Solicitante" type="xsd:string"/>
            <xsd:element name="motivo" type="MotivoOposicion"/>
            <xsd:element name="acredito" type="xsd:string" />
        </xsd:sequence>
      </xsd:complexType>
      <xsd:simpleType name="MotivoOposicion">
        <xsd:restriction base="xsd:string">
          <xsd:enumeration value="INTERESPUBLICO"/>
          <xsd:enumeration value="INTERESLEGITIMO"/>
          <xsd:enumeration value="INTERESESTADISTICO"/>
        </xsd:restriction>
      </xsd:simpleType>
      <xsd:complexType name="OposicionResponse">
        <xsd:sequence>
          <xsd:element name="Resultado" type="Resultado" minOccurs="0"/>
        </xsd:sequence>
      </xsd:complexType>
      <xsd:complexType name="Supresion">
        <xsd:sequence>
            <xsd:element name="Solicitante" type="xsd:string"/>
        </xsd:sequence>
      </xsd:complexType>
      <xsd:complexType name="SupresionResponse">
        <xsd:sequence>
          <xsd:element name="Resultado" type="Resultado" minOccurs="0"/>
        </xsd:sequence>
```

```
    </xsd:complexType>
    <xsd:complexType name="Limitacion">
      <xsd:sequence>
          <xsd:element name="Solicitante" type="xsd:string"/>
          <xsd:element name="motivo" type="MotivoLimitacion"/>
      </xsd:sequence>
    </xsd:complexType>
    <xsd:simpleType name="MotivoLimitacion">
      <xsd:restriction base="xsd:string">
        <xsd:enumeration value="ILICITO"/>
        <xsd:enumeration value="RECLAMACION"/>
      </xsd:restriction>
    </xsd:simpleType>
    <xsd:complexType name="LimitacionResponse">
      <xsd:sequence>
        <xsd:element name="Resultado" type="Resultado" minOccurs="0"/>
      </xsd:sequence>
    </xsd:complexType>
    <xsd:complexType name="Portabilidad">
      <xsd:sequence>
        <xsd:element name="Solicitante" type="xsd:string"/>
        <xsd:element name="Destino" type="xsd:string"/>
      </xsd:sequence>
    </xsd:complexType>
    <xsd:complexType name="PortabilidadResponse">
      <xsd:sequence>
        <xsd:element name="Resultado" type="Resultado" minOccurs="0"/>
      </xsd:sequence>
    </xsd:complexType>

    <xsd:complexType name="DecisionesAutomatizadas">
      <xsd:sequence>
          <xsd:element name="Solicitante" type="xsd:string"/>
      </xsd:sequence>
    </xsd:complexType>
    <xsd:complexType name="DecisionesAutomatizadasResponse">
      <xsd:sequence>
        <xsd:element name="Resultado" type="Resultado" minOccurs="0"/>
      </xsd:sequence>
    </xsd:complexType>
    <xsd:complexType name="Resultado">
      <xsd:sequence>
        <xsd:element name="Observations" type="xsd:string"/>
        <xsd:element name="DatosPersonales" type="DatosPersonales" minOccurs="0"/>
      </xsd:sequence>
    </xsd:complexType>
    <xsd:complexType name="DatosPersonales">
      <xsd:sequence>
        <xsd:element name="InformacionDatosPersonales" type="InformacionDatosPersonales"/>
        <xsd:element name="FinesTratamiento" type="xsd:string"/>
        <xsd:element name="Categorias" type="xsd:string"/>
        <xsd:element name="Destinatarios" type="xsd:string"/>
        <xsd:element name="PlazoConservacion" type="xsd:string"/>
        <xsd:element name="GarantiasTransferenciaInternacional" type="xsd:string"/>
        <xsd:element name="DecisionesAutomatizadas" type="xsd:string"/>
        <xsd:element name="Origen" type="xsd:string"/>
      </xsd:sequence>
    </xsd:complexType>
    <xsd:complexType name="InformacionDatosPersonales">
      <xsd:sequence>
        <xsd:any minOccurs="0"/>
      </xsd:sequence>
    </xsd:complexType>
</xsd:schema>
```