PA131-02-DatCiudadano

S1581: SOLUCIÓN INFORMÁTICA DE GESTIÓN DE DATOS PERSONALES DEL CIUDADANO COLOMBIANO

CARLOS ANDRÉS CAMARGO BEDOYA

PONTIFICIA UNIVERSIDAD JAVERIANA
FACULTAD DE INGENIERIA
MAESTRÍA EN INGENIERÍA DE SISTEMAS Y COMPUTACIÓN
BOGOTÁ, D.C.
2014

PA131-02-DatCiudadano
S1581: SOLUCIÓN INFORMÁTICA DE GESTIÓN DE DATOS PERSONALES DEL CIUDADANO COLOMBIANO

Autor:

Carlos Andrés Camargo Bedoya

MEMORIA DEL TRABAJO DE GRADO REALIZADO PARA CUMPLIR UNO DE LOS REQUISITOS PARA OPTAR AL TITULO DE

MAGÍSTER EN INGENIERÍA DE SISTEMAS Y COMPUTACIÓN

Director

Ing. Lina María Consuelo Franky de Toro PhD

Comité de Evaluación del Trabajo de Grado

Jeimy José Cano Martínez

Rafael Vicente Páez Méndez

Página web del Trabajo de Grado

http://pegasus.javeriana.edu.co/~PA131-02-DatCiudadano/

PONTIFICIA UNIVERSIDAD JAVERIANA
FACULTAD DE INGENIERIA
MAESTRÍA EN INGENIERIA DE SISTEMAS Y COMPUTACIÓN
BOGOTÁ, D.C.
Enero, 2014

PONTIFICIA UNIVERSIDAD JAVERIANA
FACULTAD DE INGENIERIA
CARRERA DE INGENIERIA DE SISTEMAS

Rector Magnífico

Joaquín Emilio Sánchez García S.J.

Decano Académico Facultad de Ingeniería

Ingeniero Jorge Luis Sánchez Téllez

Decano del Medio Universitario Facultad de Ingeniería

Padre Antonio José Sarmiento Nova, S.J.

Director Maestría en Ingeniería de Sistemas y Computación

Ingeniero Enrique González Guerrero

Director Departamento de Ingeniería de Sistemas

Ingeniero Rafael Andrés González Rivera

Artículo 23 de la Resolución No. 1 de Junio de 1946

"La Universidad no se hace responsable de los conceptos emitidos por sus alumnos en sus proyectos de grado. Sólo velará porque no se publique nada contrario al dogma y la moral católica y porque no contengan ataques o polémicas puramente personales. Antes bien, que se vean en ellos el anhelo de buscar la verdad y la Justicia"

AGRADECIMIENTOS

Le agradezco a Dios por acompañarme y guiarme a lo largo de mi vida, por ser mi fortaleza en momentos de debilidad, iluminar mi camino y darme el valor de asumir nuevos retos.

Le doy infinitas gracias a mi esposa Claudia y mi hijo Juan Esteban que con su paciencia y amor incondicional han acompañado este ciclo de mi vida; jamás encontraré la forma de agradecer su apoyo, comprensión y confianza. Mis logros son también suyos e inspirados en mí familia, hago de este un triunfo y quiero compartirlo por siempre con ustedes.

A mi directora de tesis, Ing. Lina María Consuelo Franky de Toro por su esfuerzo y dedicación, quien con sus conocimientos, su experiencia, su paciencia y su motivación me oriento y acompaño en el desarrollo de este trabajo de grado bajo los principios de excelencia y calidad.

A Carlos Enrique Salazar Muñoz y Aida Lucia Hurtado Bejarano de la Superintendencia de Industria y Comercio por su disponibilidad, orientaciones, recomendaciones, aportes y participación activa en el desarrollo de este trabajo de grado.

A Oscar Almanza Rodríguez, José Ricardo Aponte Oviedo y Julio Cesar Mancipe Caicedo de Gobierno en Línea, por sus comentarios y recomendaciones.

Agradecer hoy y siempre a mi familia por el esfuerzo realizado por ellos. A mi abuela Margarita, mi padre Marco Antonio, mi hermana Ángela, mi tío Guillermo, y demás familiares ya que me brindan el apoyo, la alegría y me dan la fortaleza necesaria para seguir adelante.

A la Pontificia Universidad Javeriana, por ser mí segundo hogar y permitirme desarrollar a nivel académico, laboral y profesional. Gracias por apoyarme en la realización de mis estudios.

A Nelson Gómez por confiar en mí, por su colaboración, paciencia y apoyo en lo laboral y en la ejecución de la Maestría, pero sobre todo por su amistad.

A mis amigos a quienes les quisiera agradecer su amistad, consejos, apoyo, ánimo y compañía en los momentos más difíciles de mi vida.

Y a todas aquellas personas que de una u otra forma me han acompañado en el desarrollo de este trabajo de grado.

A todos Gracias.

Contenido

Lista de figuras

Lista de tablas

ABSTRACT

The sensitivity of personal data and the uses to which they are subjected pose challenges for adequate protection; globally, there are regulations to protect citizens against the misuse of their personal information; Colombia has the law 1581 of 2012 on "Privacy Policy".

In this project, the "Information management solution of personal information of Colombian citizens" S1581 was developed with the objective to facilitate citizens through the use of technology, control their personal information from the perspective of exercising their right to self-determination Informed, and the right of Habeas Data. The information management solution aims to bring citizens to entities with unified access to your information including appropriate authentication mechanisms and security processes.

RESUMEN

La sensibilidad de los datos personales y los usos a que son sometidos plantean retos para su adecuada protección. A nivel mundial existen normativas a fin de proteger a los ciudadanos frente al uso inadecuado de sus datos personales; Colombia cuenta con la ley 1581 de 2012 sobre "Protección de datos personales".

En este proyecto se desarrolló "S1581: Solución informática de gestión de datos personales del ciudadano colombiano", con el objetivo de facilitar a los ciudadanos mediante el uso de tecnología, el controlar sus datos personales desde la perspectiva de ejercer su derecho a la Autodeterminación Informada y el derecho de Hábeas Data. La solución informática pretende acercar al ciudadano a las entidades con procesos unificados de acceso a su información incluyendo mecanismos apropiados de autenticación y seguridad.

RESUMEN EJECUTIVO

El manejo de la información ha cobrado una importancia vital con el avance de las tecnologías; la sensibilidad de los datos y los usos a que son sometidos plantean nuevos retos para su adecuada protección. En la vida cotidiana los ciudadanos entregan sus datos personales en innumerables situaciones y a distintas entidades, lo cual los hace vulnerables frente a usos ilegítimos de la información. Basta con dar una ojeada a la historia para encontrar situaciones específicas en donde los datos de las personas han sido utilizados para fines poco ortodoxos, entre otros los de señalamiento y discriminación masiva que han traído terribles consecuencias para la humanidad[1].

Ante los peligros que esto conlleva, los gobiernos de todo el mundo han adelantado leyes y reglamentaciones a fin de proteger a los ciudadanos frente al uso inadecuado de los datos, siendo Colombia uno de los países de Latinoamérica con grandes avances al respecto al definir en la Constitución Política de 1991 el derecho de hábeas data[2] en el artículo 15:

> "*Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas."*

Colombia da otro gran salto al respecto con la generación de la ley 1581 de 2012 sobre "Protección de datos personales"[3], junto con el decreto reglamentario 1377 de 2013[4], que describen en materia de protección de datos personales: derechos de los ciudadanos, los lineamientos del tratamiento de datos, los deberes de los responsables y encargados de los datos personales, entre otros.

Para ilustrar la problemática identificada, asumamos que un ciudadano ha decidido cambiar su primer apellido; en primera instancia realiza el procedimiento en la Registraduría Nacional del Estado Civil; posteriormente realiza el cambio en las entidades financieras con las cuales tiene una relación vigente; posiblemente también haga lo propio en el trabajo o el lugar de estudio, y con algunas otras entidades de las cuales requiere productos o servicios. Ahora ¿cómo podría este ciudadano conocer qué otras entidades pueden tener sus datos personales?; aun así, si las conociera, ¿cómo puede tener la seguridad que su nuevo nombre ya se ha reflejado en dichas entidades y es correcto? ¿Puede saber que él dio su autorización para que traten su información?

Se requeriría que el ciudadano acudiera a cada entidad solicitando mediante procesos diferentes el detalle de sus datos y luego radicar una solicitud de rectificación en caso que fuera necesario. Este panorama puede generar que la información solo sea actualizada en las entidades más relevantes para el ciudadano y que él desista de ejercer su derecho con el resto de responsables.

Teniendo en cuenta la problemática planteada anteriormente, en este trabajo se desarrolló "S1581: SOLUCIÓN INFORMÁTICA DE GESTIÓN DE DATOS PERSONALES DEL CIUDADANO COLOMBIANO" con el ánimo de facilitar a los ciudadanos mediante el uso

de tecnología, el poder controlar sus datos personales. Esta solución informática permite al ciudadano identificar, consultar y solicitar actualización o rectificación a las entidades nacionales que tienen bases de datos en las cuales está su información personal.

El ciudadano de esta manera puede tener un panorama más amplio de dónde pueden estar sus datos personales, así mismo acceder a un procedimiento centralizado y unificado, dispuesto por las entidades, para consulta del detalle de su información y así evitarle conocer la casuística y procedimientos particulares de cada entidad para ejercer sus derechos.

La solución S1581 permite al ciudadano acceder a funcionalidades como: consulta de entidades que tratan sus datos personales, consulta de información de contacto y aviso de privacidad de una entidad, consulta del detalle de los datos personales que posee una entidad específica, generación de solicitudes de rectificación de datos y de revocación de autorización.

Dentro de la ejecución del proyecto se desarrolló una propuesta de taxonomía de datos personales, la cual pretende ser una orientación para las entidades en la clasificación de los datos que poseen de los ciudadanos. En la solución informática al ir al detalle de los datos es posible consultarlos de acuerdo a su jerarquía, teniendo en cuenta la clasificación realizada por la entidad; lo anterior se realiza desde un elemento especial llamado componente de navegación taxonómica, su objetivo es el de dar al ciudadano una visión de cómo se estructuran sus datos personales, facilitar la consulta e identificación de datos y mejorar la experiencia de usuario.

Desde la perspectiva de tecnología, como parte de la arquitectura de la solución S1581 se desarrollaron e implementaron los siguientes ítems: mecanismos multinivel de autenticación del ciudadano; seguridad entre componentes, utilizando cifrado de canal y autenticación dual entre la solución y los servicios de información; especificación de interfaces de integración de los componentes, incluyendo la descripción de los procesos de consulta de información personal; desarrollo de portal web. Algunas de las tecnologías utilizadas dentro del desarrollo del proyecto son: JEE6[5], MySQL[6], JSON[7], Certificados Digitales (OpenSSl, keytool)[8], OpenID[9], Web Services (JAX-WS) [10], JBoss Aplicaction Server[11], entre otras.

Con el objetivo de validar la solución informática en el contexto de una entidad real que almacena información personal, se realizó un proceso de análisis en la Pontificia Universidad Javeriana; desde la perspectiva técnica se realizó la integración con el sistema principal de gestión de procesos académicos y administrativos (en ambiente de pruebas), y desde la perspectiva funcional se realizó un proceso de revisión de percepción de la solución con encargados de TIC´s de la institución.

Del trabajo realizado con la Universidad Javeriana se resalta el corto tiempo en que se pudo implementar el servicio de información en la institución y la flexibilidad para presentar los datos personales. De otra parte se identificaron retos como el de concientizar a las altas directivas para apoyar iniciativas de protección de datos y la generación de la clasificación de los datos personales; en el mismo sentido, se obtuvieron oportunidades de mejora a nivel técnico, como incluir el soporte de tipos de datos estructurados, datos multi-valor y manejo de formatos de fecha

Dentro del proyecto se contó con el acompañamiento de la Superintendencia de Industria y Comercio (SIC), autoridad en la protección de datos personales en Colombia, a través de la Dirección de Investigación de Protección de Datos Personales. La solución fue presentada a esta dependencia con quienes se validó el alcance del proyecto, las oportunidades de implementación, impactos potenciales y la posible aceptación por parte de los actores involucrados (ciudadanos y entidades).

En la validación con la SIC, la solución informática tuvo una buena aceptación como iniciativa para facilitar a los ciudadanos ejercer sus derechos; los entrevistados resaltaron los elementos de seguridad tenidos en cuenta y la facilidad de uso de la herramienta. De igual manera indicaron que una solución de este tipo genera un nivel de responsabilidad muy alto, ya que algún defecto o falencia en aspectos tales como la autenticación y privacidad del ciudadano conllevarían a incurrir en faltas contra la ley. De otra parte hicieron énfasis en que en una implementación nacional se pueden encontrar barreras como la falta de voluntad de las entidades para acoger la solución y la necesidad de posibles reformas a la ley. Los consultados perciben que la solución puede ser ampliamente aceptada por las entidades para una implementación local, que les permitiría sobrepasar retos como la integración de sus sistemas y así agilizar el cumplimiento de la ley.

INTRODUCCIÓN

La constitución colombiana de 1991 reconoce en el artículo 15 el derecho de cualquier persona a su intimidad personal y familiar, y a su buen nombre[2], ésto enmarca las garantías que tienen los ciudadanos para hacer respetar su privacidad y mantener su reputación. En el ámbito de las relaciones sociales, políticas y comerciales el ingrediente principal es "información", es así que también establece que los ciudadanos "*tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellos en bancos de datos y en archivos de entidades públicas y privadas*"[2].

Son varios los esfuerzos a nivel mundial para proteger la información personal; Europa tiene un amplio recorrido en esta área, es así como España celebra "20 años de protección de datos" aludiendo a la entrada en vigor de "Ley Orgánica de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal (LORTAD)" hoy derogada por la actual "Ley Orgánica de Protección de Datos (LOPD)"[12] [13].

Colombia por su parte en el año 2008 estableció la Ley 1266, conocida como "LEY DE HABEAS DATA", que tiene por objeto desarrollar el derecho constitucional establecido en los artículos 15 y 20 de la constitución política, en los cuales se protegen "derechos, libertades y garantías constitucionales relacionadas con la recolección, tratamiento y circulación de datos personales"[14], específicamente para la información de carácter financiero y crediticio, comercial, de servicios y proveniente de terceros países[14][15].

Para proteger la información personal que está fuera del ámbito financiero, se dio origen a la LEY 1581 de 2012, por la cual se dictan disposiciones generales para la "Protección de datos personales"[3] y cobija cualquier información registrada en una base de datos o que sea objeto de tratamientos, tales como la recolección, almacenamiento, uso, circulación o supresión[3][4].

A pesar de que las leyes han sido sancionadas, algunas de las problemáticas surgen al intentar implementarlas. Algunos sistemas o bases de datos han nacido para dar respuesta a las necesidades de negocio, no obstante, presentan carencias significativas en el ámbito de la seguridad y la privacidad.

Las entidades deberían preocuparse por apropiar el concepto de "*Privacy by Design* (PbD)"[16][17], como lo indica Ann Cavoukian, "Los principios de Privacidad por Diseño pueden ser aplicados a todos los tipos de información personal". PbD promueve que la privacidad debe ser contemplada como una configuración predeterminada, en la cual se incluye medidas preventivas y proactivas que anticipan eventos de invasión de privacidad[16].

Cesar Villamizar, Investigador de la Dijín[18], sugiere que el ciudadano debe preocuparse por mantener el control de su información e indica que hace falta una institución, entidad o herramienta que permita identificar dónde están y quién tiene los datos personales. En Colombia la ley 1581 de 2012 faculta a la Superintendencia de Industria y Comercio como "la autoridad de protección de datos", y contempla la creación de un registro único de bases de datos (RNBD)[3]. Sin embargo, esta aproximación no contempla el conocimiento e identifi-

cación de quién tiene los datos personales de un ciudadano específico, ya que el alcance del RNBD es el de actuar como un directorio público en donde se encontrarán las políticas de tratamiento de datos personales y la información de contacto de cada entidad.

La puesta de valor de "S1581: Solución informática de gestión de datos personales del ciudadano colombiano", producto del presente proyecto, es la de facilitar a los ciudadanos mediante el uso de tecnología, el controlar sus datos personales desde la perspectiva de ejercer su derecho a la Autodeterminación Informada y el derecho de Hábeas Data. La solución S1581 pretende acercar al ciudadano a las entidades con procesos unificados de acceso a su información, e incluyendo mecanismos apropiados de autenticación y seguridad para el tratamiento de sus datos personales.

El presente documento se ha organizado de la siguiente manera: El capítulo I comprende una descripción general del proyecto, en donde se presentan el problema u oportunidad de mejora identificada, los objetivos y la metodología utilizada para el proyecto. Enseguida en el capítulo II se encuentra el marco contextual, en donde se describe el panorama de protección de datos en el mundo. Posteriormente en el capítulo III marco teórico se aborda los conceptos, tecnologías y herramientas que soportan el desarrollo de la solución S1581. El capítulo IV presenta los detalles del desarrollo del proyecto donde se profundiza en elementos como las funcionalidades, taxonomía de datos personales, diseño de la solución, arquitectura y especificación de integraciones, descripción de solución informática S1581 y validación del proyecto. Finalmente, se incluye en el capítulo V las conclusiones y trabajo futuros.

I - PRESENTACIÓN DEL TRABAJO DE GRADO

En este capítulo se describe el problema u oportunidad de mejora, los objetivos del proyecto y el potencial de innovación de la solución S1581.

1. Problemática u oportunidad de mejora.

Desde el punto de vista del ciudadano, existen algunas situaciones que pueden dificultar la gestión y control de sus datos personales, provocando que se desista de este propósito. Entre otros casos, la ley faculta al ciudadano para hacer exigencias de actualización y rectificación de datos personales[3]; a pesar de esto, el usuario común probablemente no conoce todas las entidades en donde pueda estar su información[18].

Otra dificultad surge porque la consulta de datos se debe realizar en cada entidad [8], lo que involucra diferentes mecanismos y procedimientos de acceso a la información. El individuo también se enfrentará a volúmenes considerables de datos; la verificación de integridad y veracidad pueden tornarse complejos, puesto que el mismo dato puede presentar, de acuerdo al repositorio, diferencias tales como escritura, formato, completitud y orden.

Estas problemáticas presentan retos tecnológicos como la integración de plataformas no homogéneas, la generación de mecanismos de autenticación y autorización, y la construcción de interfaces amigables. Para el préstamo de servicio en línea la autenticación de los ciudadanos es un reto significativo, dado que no existe un usuario o contraseña pre-establecidos para cada individuo; por el contrario, si no existe una validación rigurosa se puede estar entregando información a personas no autorizadas, incumpliendo con los principios de privacidad y confidencialidad. Se requiere por lo tanto encontrar una solución que permita la identificación del ciudadano mediante mecanismos acordes al riesgo de acceder a funcionalidades que interactúan con información personal.

La motivación de este trabajo de grado se enfoca en el ánimo de facilitar a los ciudadanos mediante el uso de tecnología, el poder de controlar sus datos personales desde la esencia misma del derecho de la Autodeterminación Informada[1] y el derecho de Hábeas Data. Con esta visión se pretende que el ciudadano pueda tener un panorama más amplio de dónde pueden estar sus datos personales; así mismo esta iniciativa pretende generar un procedimiento centralizado y unificado que puedan seguir las entidades para prestar el servicio para consultar el detalle de datos personales y así evitar al ciudadano tener que conocer la casuística de cada entidad y cada uno de los procedimientos disponibles para ejercer sus derechos.

[1] Los derechos de Autodeterminación Informada y Hábeas Data son explicados en la sección Marco Contextual.

Teniendo en cuenta elementos de la Ley 1581 de 2012 y del decreto 1377 de 2013 se han identificado oportunidades de mejora o posible aplicación de tecnología sobre elementos tales como[2]:

1. Artículo 8°. Derechos de los Titulares
    a. Conocer, actualizar y rectificar sus datos personales frente a los Responsables del Tratamiento o Encargados del Tratamiento.
    b. Acceder en forma gratuita a sus datos personales que hayan sido objeto de Tratamiento.
    c. Ser informado por el Responsable del Tratamiento o el Encargado del Tratamiento, previa solicitud, respecto del uso que le ha dado a sus datos personales.
    d. Revocar la autorización y/o solicitar la supresión del dato.
2. Artículo 11. Suministro de la información.
    a. La información solicitada podrá ser suministrada por cualquier medio, incluyendo los electrónicos.
    b. La información deberá ser de fácil lectura, sin barreras técnicas que impidan su acceso.
3. Artículo 12. Deber de informar al Titular.
    a. El Tratamiento al cual serán sometidos sus datos personales y la finalidad del mismo;
4. Decreto Reglamentario, Artículo 21 Del derecho de acceso.
    a. Los Responsables y Encargados del Tratamiento deben establecer mecanismos sencillos y ágiles que se encuentren permanentemente disponibles a los Titulares con el fin de que estos puedan acceder a los datos personales que estén bajo el control de aquéllos y ejercer sus derechos sobre los mismos.
5. Decreto Reglamentario, Artículo 27 Políticas internas efectivas
    a. Adopción de procesos para la atención y respuesta a consultas, peticiones y reclamos de los Titulares, con respecto a cualquier aspecto del Tratamiento.

El desarrollo de una solución informática de este tipo también se enfrenta a retos impuestos por la misma ley dado que requiere tratar datos personales, estos son algunos de ellos:

1. Como lo indica el Artículo 13 las Personas a quienes se les puede suministrar la información son los Titulares, sus causahabientes o sus representantes legales.
2. De acuerdo al decreto reglamentario los derechos podrán ejercerse por el Titular, quien deberá acreditar su identidad en forma suficiente por los distintos medios que le ponga a disposición el responsable.
3. Como lo indica el artículo 11 del decreto reglamentario los datos personales se deberán manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

[2] Los siguientes ítems se han extraído textualmente de la Ley 1581 de 2012 o del decreto reglamentario 1377 de 2013 con el objeto de mostrar la motivación que inspiraron este trabajo de grado.

2. Objetivos

De acuerdo a las problemáticas identificadas se plantearon para este proyecto un objetivo general y siete objetivos específicos; a continuación se describe cada uno de ellos.

2.1. Objetivo General

Construir, bajo el marco de la ley 1581 de 2012 sobre "Protección de datos personales"[3], una solución informática que permita al ciudadano colombiano, identificar, consultar y solicitar actualización o rectificación a las entidades nacionales que tienen bases de datos en las cuales está su información personal.

2.2. Objetivos Específicos

1. Identificar funcionalidades que faciliten al ciudadano ejercer los derechos estipulados en la ley 1581 de 2012, tales como "conocer, actualizar y rectificar" su información personal[3].

2. Diseñar la arquitectura de la solución informática a implementar.

3. Diseñar y especificar interfaces de integración, que describan la interacción entre la solución informática y las entidades que gestionan datos personales.

4. Implementar una solución informática que cumpla con las funcionalidades seleccionadas.

5. Implementar un mecanismo de autenticación apropiado para la identificación adecuada del ciudadano.

6. Validar la solución informática, mediante la integración con una entidad real que almacene información personal.

7. Validar los resultados obtenidos ante una autoridad o entidad de gobierno que sea actor en la aplicación de la Ley de Protección de Datos.

3. Metodología

La construcción de la solución de gestión de datos personales del ciudadano colombiano (S1581), se dividió en 4 fases: definición de funcionalidades, definición de arquitectura, desarrollo de solución informática S1581 y desarrollo de integración con una entidad real que almacene información personal.

La implementación de la solución fue orientada por la metodología ágil, *Extreme Programming (XP)*[19]; la cual permitió realizar un desarrollo de manera incremental, flexible a los cambios. En la Figura 1 se ilustra el ciclo de vida de implementación de la solución. A continuación se describe cada una de las fases.

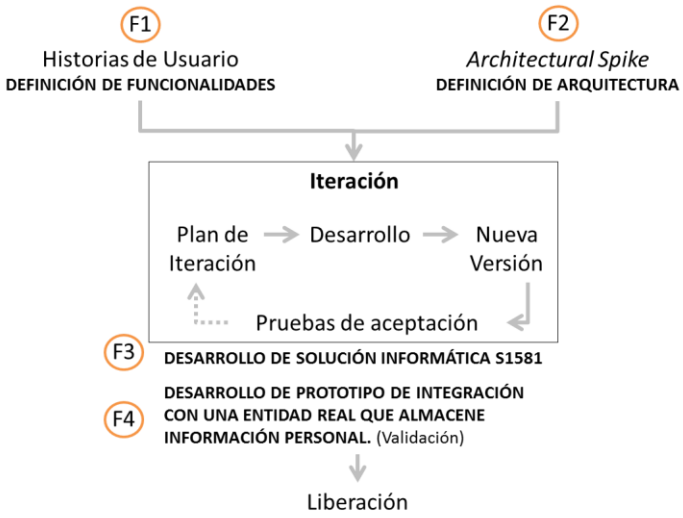

Figura 1. Ciclo de vida de proyecto S1581. Adaptado de metodología XP [20].

Fase 1. Definición de funcionalidades: En esta fase se establecieron los requerimientos del sistema, obteniendo como resultado las funcionalidades que fueron incluidas en la solución. Estos requerimientos se gestionados de acuerdo a la metodología *XP* con lo que se denomina "Historias de Usuario"[21]. Se contemplan las siguientes actividades:

a. Búsqueda y análisis de Información, en relación a la Protección de Datos Personales.
b. Descripción de funcionalidades identificadas, en forma de historias de usuario.
c. Definición de criterios de selección de funcionalidades.
d. Selección de funcionalidades.

Fase 2. Definición de arquitectura: La fase de definición de arquitectura se adordo teniendo en cuenta el concepto de *XP* denominado "*Architectural Spike*"[20]. De esta manera, se identificaron tecnologías que contribuían a la construcción de la plataforma; se realizó un estudio de estos elementos para conocer características como comportamiento, diseño o funcionalidad.

El resultado en este punto, fue la descripción de los componentes arquitectónicos que guiaron el desarrollo de la solución informática S1581; también se contempló la especificación de interfaces de integración, la cual definió los protocolos, datos, tecnologías y demás aspectos que se requerirán para la comunicación entre la solución S1581 y las entidades que gestionan datos personales. Para el desarrollo de esta fase se realizaron las siguientes actividades:

a. Exploración y análisis de tecnologías.
b. Selección de tecnologías.
c. Definición de la arquitectura.
d. Documentación de la arquitectura.
e. Definición de interfaces de integración.
f. Documentación de interfaces de integración.

Fase 3. Desarrollo de solución informática S1581: La fase 3 incluyo varias iteraciones de acuerdo a la metodología propuesta, en ella se realizaron las actividades enfocadas a desarrollo y pruebas para obtener la solución informática S1581. Para el desarrollo de esta fase se realizaron las siguientes actividades:

a. Planeación de la iteración.
b. Definición e Implementación de pruebas.
c. Desarrollo de la solución informática S1581.
d. Ejecución de Pruebas.
e. Documentación técnica de la solución.
f. Verificación y validación con Superintendencia de Industria y Comercio.

Fase 4. Desarrollo de prototipo de integración con una entidad real que almacene información personal: La fase final, abarcó actividades enfocadas a verificar la solución de software, mediante la implementación de la integración con una entidad real que gestiona datos personales. En este proyecto se contó con el apoyo de la Pontificia Universidad Javeriana. Se incluyó en esta fase también actividades de verificación de la solución con la superintendencia de industria y comercio. Para el desarrollo de esta fase se realizaron las siguientes actividades:

a. Selección de entidad real que almacena datos personales.
b. Identificación de repositorio de datos personales de la entidad real.
c. Planeación de la iteración.
d. Definición de pruebas.
e. Desarrollo de las Interfaces de integración.
f. Ejecución de Pruebas.
g. Documentación técnica de la integración.
h. Verificación y validación con entidad.

4. Potencial de Innovación

El desarrollo del proyecto, contempla dos frentes en los cuales se prevé un aporte significativo. Por una parte, si el Estado establece una plataforma como S1581, facilitará a los ciudadanos el acceso a la información, reducirá las necesidades de capacitación y disminuirá los tiempos requeridos para gestionar la información personal, lo cual beneficiará al ciudadano. Este modelo podría ser exportado a países que estén interesados en apoyar tecnológicamente sus políticas de protección de datos personales.

Por otra parte, si las entidades apropian esta tecnología se verán favorecidas con la implantación de un producto que desde su concepción vincula los principios de “Privacy by design” y de protección de datos personales. Así mismo, la entidad que desarrolle la interfaz de integración propuesta en este proyecto podrá cumplir rápidamente con algunos de los deberes establecidos en la ley 1581 de 2012 que son exigidos a partir de abril de 2013 y así evitar posibles sanciones. A futuro la plataforma podrá complementarse con actividades consultivas que ayuden en la implementación de la ley.

II - MARCO CONTEXTUAL

En este capítulo se profundiza en la definición de dato personal y como se aborda desde el punto de vista normativo su protección. Se incluye una breve revisión de las normas de protección de datos personales en diferentes regiones del mundo.

1. El dato personal

Todo individuo, como lo menciona Alberto Bianchi, "está rodeado de características, estados y situaciones que lo conforman"[22]; una persona cuenta con un nombre, apellido, un domicilio, un estado civil, estado de salud, relaciones financieras y crediticias, creencias religiosas, preferencias sexuales, entre otros. Esta información al ser parte de un registro se convierte en datos mediante los cuales se puede llegar a conocer, identificar o discriminar a las personas[22]. Todo esto es conocido como datos personales.

De acuerdo a la resolución de Madrid de 2009[23] se define como Dato de Carácter Personal a "*cualquier información concerniente a una persona física identificada o que pueda ser identificada a través de medios que puedan ser razonablemente utilizados*." Por su parte la *United States Government Accountability Office (GAO)* y la *National Institute of Standards and Technology (NIST)*, referencia los datos personales como "Información de identificación Personal"[3] (PII por sus siglas en inglés)[24] y la definen como: "*Cualquier información acerca de un individuo gestionada por una agencia, incluyendo (1) cualquier información que pueda ser usada para distinguir o seguir la identidad de un individuo,…cualquier otra información que vincule o asocie a un individuo* "[25].

Los datos personales pasan por una serie de operaciones y procedimientos como la obtención, conservación, almacenamiento, modificación, transformación, evaluación, destrucción y cesión a terceros; el conjunto de estas acciones es conocido como tratamiento de datos personales[26].

El entorno de las nuevas tecnologías ha permitido ampliar las fronteras del tratamiento de los datos personales, actualmente se cuenta con mecanismos que permiten obtener rápidamente información personal, enormes capacidades de almacenamiento, redes de alta velocidad que permiten una rápida difusión y una alta gama de dispositivos que facilitan el acceso. Es así que Mario Masciotra[26] señala los siguientes peligros para la información personal:

a. Acceso de manera ilimitada y sin restricciones por parte de las autoridades.
b. Tratamiento de datos sensible, los cuales hacen referencia a cuestiones íntimas de las personas; por ejemplo, religión, raza, ideología, opinión política, posición filosófica, tendencias psicológicas, tendencias sexuales, situaciones familiares y parentales, entre otras.[26].

[3] En el presente documento se utilizará el término información personal para referirse también a datos personales.

c. Tratamiento de datos sin consentimiento del individuo o titular.
d. Utilización de la información con fines distintos para los que fueron obtenidos.
e. La inferencia de datos privados al entrelazar distintos datos de carácter público.
f. La permanencia de los datos así no se requieren para los fines autorizados.
g. Dificultad para que los titulares de los datos personales tengan conocimiento de donde y quien trata su información personal.
h. Dificultad para que el titular pueda solicitar corrección, modificación o supresión de sus datos personales.

A lo anterior se añade el poco interés de los titulares en gestionar su información personal y custodiarla de manera adecuada. Aun así existe una gran preocupación por el tratamiento de los datos personales, NIST en el documento "*Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*" indica que la problemática está en que la Información de Identificación Personal (PII) "*debe ser protegida contra el acceso, uso y divulgación inapropiados*"[24]. Diferentes gobiernos del mundo han desarrollado normativas que procuran proteger al ciudadano frente a terceros, en el uso inapropiado de sus datos personales.

En la siguiente sección se presenta la historia y el panorama de la protección de datos personales en distintas regiones del mundo.

2. Protección de datos personales en Europa

En la década de los años 40´s en Europa, se presentó una grave falta a la intimidad y privacidad de las personas, en Alemania se utilizó la información de los archivos nacionales y del censo de 1933 para identificar a los ciudadanos judíos y someterlos a hechos lamentables que terminaron en el genocidio[1]. Una vez terminada la Segunda Guerra Mundial se desarrollaron iniciativas que pretendían proteger a los ciudadanos frente a actos que atentaran contra la intimidad y la vida privada. En la DECLARACIÓN UNIVERSAL DE DERECHOS HUMANOS de 1948 se incluye en el artículo 12 la protección sobre injerencias a la vida privada y la familia, así como de ataques contra la honra o reputación[27].

La constitución alemana de 1949 indica que "*Cada uno tendrá derecho al libre desenvolvimiento de su personalidad …*"[1] siendo este la formalización del derecho a la vida privada[1]. En 1950 el Convenio Europeo de Derechos Humanos incluye el artículo 8 sobre "Derecho al respeto a la vida privada y familiar"[28].

En los años 70´s se concretan leyes específicas en cada país sobre protección de datos personales; en 1970 Alemania sanciona la primera Ley de protección de datos, y en 1977 la Ley Federal de Protección de Datos; estas normativas fueron consideradas como una de las más estrictas del mundo[1]. Alemania es seguida por otros países como Suecia y Francia; las leyes desarrolladas incluyen la prohibición del tratamiento de los datos personales sin el consentimiento del titular, del almacenamiento ilegal de los datos personales, del almacenamiento de datos personales inexactos, y del abuso o divulgación no autorizada; también establece la creación de entidades de protección de datos y un ámbito de aplicación tanto en el sector público como el privado[1][29].

Gracias a la sentencia de 15 de diciembre 1983 del Tribual Constitucional alemán, se establece formalmente el derecho del individuo a controlar la información sobre sí mismo reconociendo la facultad del ciudadano de decidir por sí sólo sobre la difusión y utilización de sus datos personales; este derecho es conocido como "Autodeterminación informativa"[1].

La Organización para la Cooperación y el Desarrollo Económicos (OECD por sus siglas en inglés) elaboró en 1980 el documento "Directrices sobre protección de la privacidad y flujos transfronterizos de datos personales" como una forma de mitigar las diferencias entre las distintas legislaciones permitiendo la libre circulación de los datos personales a través de las fronteras[29].

Siguiendo la línea de realizar esfuerzos internacionales en el ámbito de protección de datos y en busca de establecer un marco jurídico común, en 1981 los estados miembros del consejo de Europa firman el "Convenio 108". El cual tiene por objeto "*garantizar, en el territorio de cada Parte, a cualquier persona física sean cuales fueren su nacionalidad o su residencia, el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal*" [29].El convenio 108 contempla principios básicos de la protección de datos tales como:

- Compromiso de las partes para tener internamente instrumentos que protejan los datos personales.
- Propender por la calidad de los datos, en el cual la obtención y tratamiento sean para finalidades leales y legítimas, dichas finalidades deben estar determinadas; los datos personales deben ser exactos y conservados únicamente por el periodo requerido para las finalidades previstas.
- Tratamiento especial de datos sensibles, los cuales son definidos como "Categorías particulares de datos"; se restringe el tratamiento automatizado únicamente cuando existan garantías explicitas sobre este tipo de datos.
- Se deben tomar medidas de seguridad contra la destrucción accidental o no autorizada, la pérdida accidental, así como contra el acceso, la modificación o la difusión no autorizados.
- Garantías complementarias que permite a cualquier persona conocer la existencia de los ficheros que tengan su información, de la misma manera la identidad, la residencia y establecimiento principal del responsable del fichero, así como conocer el detalle de su información; podrá también solicitar la rectificación o borrado de sus datos personales.
- Cada parte se compromete a establecer las sanciones y recursos aplicables a las infracciones de las normativas de protección de datos.

Acerca de la interacción internacional el convenio 108 indica que las disposiciones allí concebidas serán aplicadas a los flujos transfronterizos de datos de carácter personal, e involucra a los diferentes países en un ambiente de cooperación mutua que permita el cumplimiento del convenio y la asistencia a las personas que tengan su residencia en el extranjero[30]. A pesar de los esfuerzos, el convenio 108 no tuvo el impacto esperado [31] por lo que las propuestas comunitarias de protección de datos se congelaron hasta finales de la década del 80[31].

De otra parte, el 14 de Diciembre de 1990 la asamblea general de la ONU aprobó la resolución 45/95 que estableció orientaciones que deben acoger los estados miembros respecto a los reglamentos relativos a los archivos computarizados de datos personales.

Francia en 1989 revive las iniciativas europeas, proponiendo armonizar las leyes de protección de datos personales, la propuesta es acogida en 1990 con el objeto de eliminar las barreras económicas y de mercado que impone el no poder tener un tránsito libre de los datos personales por restricciones en la legislación de cada estado[1]. El Consejo de Europa entonces toma la responsabilidad de lograr una norma común; dando así origen a la "*Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos*".

La Directiva 95/46/CE tiene por objeto garantizar "*la protección de las libertades y de los derechos fundamentales de las personas físicas, y, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales.*"[32] Esta directiva precisa y amplia los principios del Convenio del 28 de enero de 1981 del Consejo de Europa para la protección de las personas en lo que respecta al tratamiento automatizado de los datos personales[32]. Esta directiva brinda definiciones para los conceptos de "datos personales", "tratamiento", "fichero", "responsable del tratamiento", "encargado del tratamiento", "tercero", "destinatario" y "consentimiento del interesado". Acerca de los principios y en comparación con el Convenio 108 incluye o describe[32][1]:

- Acerca de la calidad de los datos, ratifica que los datos deben ser tratados de manera leal y lícita. Define que los fines deben ser explícitos e incluye lineamientos para el tratamiento de datos personales con fines históricos, estadísticos o científicos.
- Describe explícitamente cuando se considera un tratamiento legítimo; referenciando que el interesado ha dado su consentimiento de forma inequívoca o que la información es necesaria para la ejecución de un contrato, el cumplimiento de una obligación jurídica, proteger el interés vital del interesado, entre otras.
- Amplia y precisa aspectos del tratamiento de categorías especiales de datos.
- Incluye lineamientos en el tratamiento de datos personales con fines exclusivamente periodísticos o de expresión artística o literaria.
- Indica la obligación de informar al interesado y describe la información que le debe ser entregada.
- Describe los derechos de acceso y oposición del interesado.
- Incluye directrices sobre confidencialidad y amplía las relativas a seguridad del tratamiento.
- Indica que los estados miembros deben disponer de autoridades de control, describe sus funciones y enmarca lineamientos de notificación de los responsables del tratamiento de los datos personales hacia estas.
- Referencia las condiciones de transferencia de datos personales a países terceros, resaltando que este tercero garantice un nivel de protección adecuado.

En el año 2000 la Carta de Derechos Fundamentales de la Unión Europea incluye explícitamente en el artículo 8 el derecho a la "Protección de datos de carácter personal" y define que

"*estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que le conciernan y a obtener su rectificación*"[33].

Desde un contexto localizado España, país reconocido por su trayectoria en la protección de datos personales, el 29 de octubre de 1992 promulgo la Ley Orgánica 5/1992 , de regulación del tratamiento automatizado de los datos de carácter personal (LORTAD)[34] que estableció el primer marco jurídico de protección de datos en ese país, posteriormente fue derogada por la Ley Orgánica de Protección de Datos 15/1999, de 13 de diciembre (LOPD)[35]. Se resalta la descripción de los derechos de acceso, rectificación, cancelación y oposición que tienen los individuos sobre los datos personales, comúnmente llamados Derechos ARCO. La experiencia española se está siguiendo como modelo en varios países latinoamericanos[36].

En 2009 se realizó la 31 Conferencia Internacional de Autoridades de Protección de Datos y Privacidad que tuvo como resultado la redacción de lo que se conoce como la Resolución de Madrid, este documento presenta una propuesta conjunta para la redacción de estándares internacionales para la protección de la privacidad en relación con el tratamiento de datos de carácter personal[23].

Finalmente, teniendo en cuenta que la tecnología ha tenido una rápida evolución que impone nuevos retos en el ámbito de la protección de datos personales, y reconociendo el enorme incremento del intercambio de datos en el desarrollo de actividades económicas, comerciales, publicas, de entretenimiento, etc. y que "las personas físicas difunden un volumen cada vez mayor de información personal a escala mundial"[37] se generó en el año 2012 la "*Propuesta de reglamento del parlamento europeo y del consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos)*"[37].

La propuesta de reglamento sigue la línea de la Directiva 95/46/CE indicando que el marco jurídico vigente es adecuado, pero haciendo hincapié en que existen riesgos significativos en el ciberespacio por lo cual pretende establecer un marco jurídico más sólido que permita "*el desarrollo de la economía digital en el mercado interior, otorgue a los ciudadanos el control de sus propios datos y refuerce la seguridad jurídica y práctica de los operadores económicos y las autoridades públicas*" [37].

3. Protección de datos personales en Estados Unidos

La protección de datos personales en Estados Unidos ha sido abordada desde el punto de vista de la protección a la privacidad, en sus inicios la célebre frase "The right to be let alone"(El derecho a ser dejado solo)[38] fue acuñada por Thomas McIntyre Cooley en 1972 a fin de dar una definición de privacidad. En 1890 Samuel Warren y Louis D. Brandeis escribieron el ensayo *The Right To Privacy* [39], con la intención de establecer mecanismos jurídicos para restringir el acceso de la prensa a cuestiones relacionadas con la vida privada de las personas; este ensayo se convertiría en una referencia para tratar los temas referentes a protección de la privacidad[1].

El desarrollo de leyes de protección de la privacidad fue impulsado por el deseo de salvaguardar al ciudadano frente al control del estado, por lo general en cuestiones que se consideran parte de la intimidad de un individuo[1]. Algunos de los eventos más relevantes hacen referencia a casos presentados ante la Corte Suprema de Justicia en la cual se luchó contra leyes tales como: prohibiciones para la enseñanza en idioma extranjero (caso Pierce *vs.* Society of Sisters[40]), prohibición del uso de anticonceptivos (caso Griswold vs. Connecticut[41]), aborto (caso Roe vs. Wade[42]), y varios temas relacionados con sexualidad; en todos estos casos la corte emitió un fallo a favor de la intimidad[1].

Explícitamente la constitución de este país y sus respectivas enmiendas no incluyen una ley de privacidad[43]; sin embargo, se da cubrimiento a esta área de manera implícita en las enmiendas primera, cuarta, quinta, novena y especial la decimocuarta[43] . En 1974 se estableció "*The privacy Act"*[44] *(Ley de privacidad)* la cual es presentada como la primera ley en este país, que reglamenta el tratamiento de información de identificación personal para las agencias federales. Existen algunas leyes que aplican a sectores específicos como por ejemplo Electronic Communications Privacy Act, de 1986, Telephone Consumer Privacy Act, 1994, Fair Credit Reporting Act, 1996[1], entre otras.

La diferencia entre la concepción de Estados Unidos y la europea radica en que no se rige específicamente sobre la protección de los datos y su propiedad, sino en la privacidad del individuo como "*la libertad de una esfera íntima*" [1]. El derecho a la privacidad "*protege los sentimientos y la sensibilidad de las personas*" [1] por lo que este derecho se puede ejercer mientras la persona tenga vida, siendo así que se extingue con la muerte; esta es otra gran diferencia con los lineamientos europeos, en los cuales se preserva el derecho a la protección de datos incluso cuando el individuo titular de los mismos ya no cuente con vida [1].

4. Protección de datos personales en Latinoamérica

Los países latinoamericanos han desarrollado de igual manera políticas de protección de datos personales, resultado de las necesidades que en este ámbito representa la evolución tecnológica, la explosión de la recolección de datos personales, los retos de ampliación de mercados y el desarrollo de la globalización[1]. Brasil incluyo en su constitución de 1988 el derecho de Hábeas Data[1], esta iniciativa fue seguida por varios países latinoamericanos[1]. Este derecho busca permitir a toda persona conocer cualquier información que le concierne en registros, archivos, bases o bancos de datos públicos y privados, asimismo solicitar su rectificación, actualización, supresión o confidencialidad[26].

Como lo indica el profesor Nelson Remolina[45] el 70% de los países latinoamericanos incluyen en sus constituciones textos referentes a la protección de datos personales, todos los países cuentan con leyes sectoriales de protección; sin embargo, solo el 40% cuenta con normas generales en la materia; se observa que las iniciativas latinoamericanas tienen una fuerte influencia Europea en el desarrollo de sus leyes generales de protección de datos personales[45][43]. La Figura 2 presenta el mapa de normas realizado por el Profesor Nelson Remolina sobre el desarrollo de la protección de datos en Latinoamérica desde 1985 a 2012.

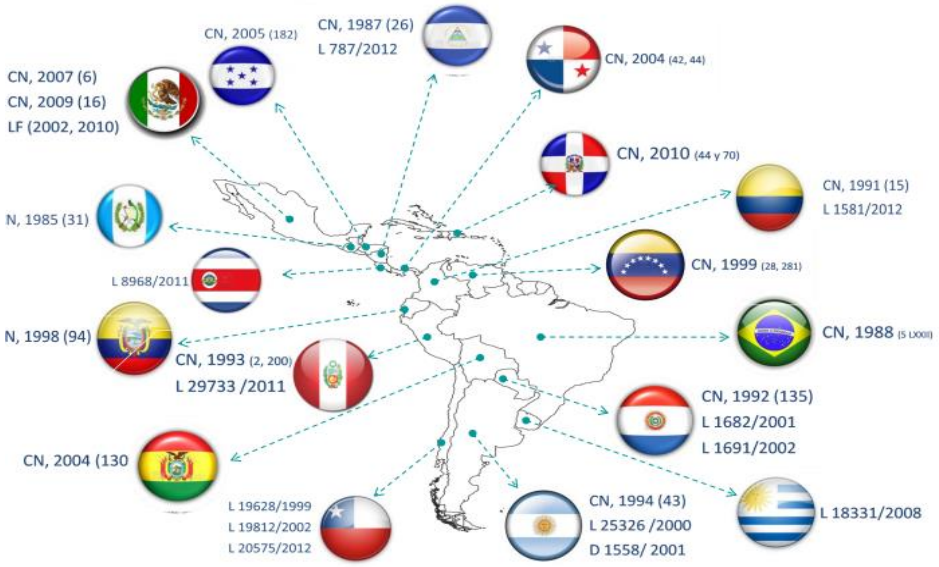

Figura 2. Mapa Latinoamericano sobre la protección de datos personales (1985-2012). Nelson Remolina Angarita ©[45].

5. Protección de datos personales en Colombia

Colombia por su parte no es ajena a las tendencias internacionales en cuestión de protección de datos personales, es así como en La Constitución Política de Colombia de 1991 se definió el derecho de hábeas data[2] en el artículo 15 como:

> "*Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas."* [2]

En el desarrollo de normas sectoriales se han incluido apartados referentes a la protección de los datos personales. Las siguientes son algunas de las más significativas[46]:

1. Ley 23 de 1981: Desarrolló las normas sobre ética médica e incluyó en el artículo 34, lineamientos sobre el carácter privado y reservado de la historia clínica[47].
2. Ley 96 de 1985: En el artículo 51 se otorgó a los datos con que cuenta la Registraduría Nacional del Estado Civil la calidad de públicos o reservados[48].
3. Ley 270 de 1996: Resalta que los procesos de administración de Justicia con soporte informático deben garantizar la confidencialidad, privacidad, y seguridad de los datos de carácter personal[49].
4. Ley 527 de 1999: Conocida como ley de Comercio Electrónico define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales; es importante en cuanto define el mensaje de datos y describe la responsabilidad de las entidades de certificación sobre los datos de los suscriptores del servicio [50].

5. Ley 1273 de 2009: Llamada Ley de Delitos Informáticos, "*crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones"*[51]*;* En esta Ley se incluyen artículos referentes a "violación de datos personales" y "suplantación de sitios web para capturar datos personales" en ambos casos se relacionan conductas sin autorización bajo el texto "sin estar facultado para ello" e impone sanciones considerables a quien incurra en dichas conductas[51].
6. Sentencia C-540/12: Se constituye como un proyecto de ley estatutaria de fortalecimiento del marco jurídico para el desarrollo de las actividades de inteligencia y contrainteligencia, incluyen apartados sobre protección de Datos Personales en ese ámbito[52].

En el año 2008 se expidió la Ley 1266 conocida como Ley de Hábeas Data Financiero, que tiene por objeto desarrollar el derecho constitucional establecido en los artículos 15 y 20 de la constitución política, en los cuales se protegen "*derechos, libertades y garantías constitucionales relacionadas con la recolección, tratamiento y circulación de datos personales*"[7], específicamente para la información de carácter financiero y crediticio, comercial, de servicios y proveniente de terceros países[7][8]. Esta Ley es parcial y sectorial[53] ya que aplica sobre datos personales relacionados con el comportamiento de obligaciones financieras[53].

La Ley 1266 de 2008 no es una norma de carácter general de Habeas Data y deja por fuera elementos contemplados en normas como la Europea, como lineamientos sobre datos de carácter especial o sensibles, derecho de oposición, entre otros[53]. Bajo este escenario se hace necesario seguir avanzando en la generación de una norma general de protección de datos personales, es así que surge la Sentencia C-748/11 que daría lugar a la Ley 1581 de 2012 por la cual se desarrolla el "*derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos*"[3] y que es parcialmente reglamentada en el decreto 1377 de 2013[4].

La ley 1581 de 2012 y el respectivo decreto reglamentario 1377 de 2013, describen en materia de protección de datos personales: derechos y condiciones de legalidad para el tratamiento de datos, deberes de los responsables y encargados del tratamiento, procedimientos para ejercer los derechos del ciudadano, definición y responsabilidades de la Autoridad de Protección de Datos Personales, sanciones, el Registro Nacional de Bases de Datos (RNBD), transferencia de datos a terceros países. Se incluye también lineamientos sobre "Categorías especiales de datos", como datos sensibles y referentes a niños, niñas y adolescentes;

Como se observa en los principios, en las definiciones, y en la totalidad del texto, la Ley 1581 está muy acorde con los lineamientos internacionales dado que Colombia por una parte debe cumplir con la resolución 45/95 de la ONU, puesto que es un país miembro de la organización; de otra parte al cumplir los estándares internacionales podría llegar a ser considerado un país adecuado por la Unión Europea en materia de Protección de Datos Personales, de conformidad con la "Directiva 95/46/CE", lo que podría favorecer las inversiones y la adopción de entidades que requieran transferencia de datos personales; actualmente solo Argentina y Uruguay tienen este reconocimiento[54][55].

III - MARCO TEÓRICO

En esta sección se describirán los referentes teóricos y conceptuales tenidos en cuenta para el desarrollo de este trabajo.

1. Privacidad por Diseño

Algunos autores como Ashbaugh[56] revelan lo que la mayoría de desarrolladores e implementadores de software y tecnología saben pero no confiesan, y es que hasta hace un tiempo la seguridad era una idea de último momento en el diseño de software[56] que incluso en ocasiones se omite[17]. Existen algunos elementos que han hecho tomar conciencia de involucrar la seguridad, en particular la que busca preservar la privacidad, de manera directa y a profundidad, no tangencialmente como se venía haciendo; encontramos por ejemplo los requisitos legales y normativos[56] tales como los exigidos por la Ley 1581 de 2012 para el tratamiento de datos personales y estándares de industria[56] tales como Payment Card Industry Data Security Standard (PCI DSS).

La Privacidad por Diseño (Privacy by Design - PbD) es un enfoque que se ha propuesto para que la privacidad y la protección de datos sea contemplada desde el inicio de cualquier iniciativa que vincule información[17]. Como lo indica Ann Cavoukian, Comisionada de Información y Privacidad de Canadá: el cumplimiento de los marcos regulatorios no debe ser la única garantía de aseguramiento de la privacidad, por lo que se busca que la protección de la privacidad sea el modo de operación de las entidades[16]. PbD es un enfoque proactivo para la protección de la privacidad que busca evitar las violaciones de datos y los perjuicios potenciales[57]. PbD contempla 7 principios fundamentales que buscan asegurar la privacidad, que los individuos tengan el control de su información personal y que las organizaciones que los apliquen tengan una ventaja competitiva[16]. Estos principios son presentados en la Figura 3.

Figura 3. Principios de Privacidad por Diseño, adaptado de [16].

PbD invita a que las medidas de robustez de la privacidad tienen que ser correspondientes a la sensibilidad de los datos tratados[16] y debe ser contemplado sobre la "trilogía"[16] que comprende sistemas de tecnologías de la información; prácticas de negocio responsables; y diseño físico e infraestructura en red[16]. Los principios de Privacidad por Diseño orientaron el desarrollo del presente proyecto en busca de incluir medidas de seguridad y de privacidad acordes a los requerimientos de la Ley, pero también tendientes a proteger a los ciudadanos y las entidades que presentan sus servicios de información bajo el principio todos ganan.

2. Control de acceso y mecanismos de autenticación

Como lo indica el Decreto 1377 de 2013 en el artículo 20, para ejercer sus derechos el titular debe "*acreditar su identidad en forma suficiente por los distintos medios que le ponga a disposición el responsable*"[4]. Esta declaración implica realizar un proceso de autenticación apropiado, en esta sección se definirá la autenticación y los diferentes mecanismos a nivel técnico que pueden ser tenidos en cuenta para el logro de este propósito.

El control de acceso es el componente de seguridad encargado de las cuestiones relativas del acceso a los recursos de un sistema por parte una persona, sistema o tercero (entidad)[8], se divide en dos aspectos principales: autenticación y autorización. La autenticación se encarga de verificar la identidad de quien está accediendo al recurso, responde a la pregunta "¿Quién anda ahí?" y toma una decisión binaria indicando si se otorga o no el acceso [8]. Por su parte la autorización, en ocasiones referida como control de acceso, protege contra la utilización de recursos por parte de entidades no autorizadas[58]; responde a la pregunta ¿Está permitido hacer eso?. En esta sección se profundiza en el concepto de autenticación dada la importancia para este proyecto.

Los métodos de autenticación pueden ser basados en uno de los siguientes 3 tipos de retos o factores[59]:

- **Algo que el usuario conoce:** Un ejemplo de este mecanismo son las contraseñas.
- **Algo que el usuario tiene:** En esta clasificación se asocian elementos externos que posee el usuario como una tarjeta inteligente, tarjeta ATM, un token, etc.
- **Algo que el usuario es:** Se asocia a características propias del usuario, normalmente rasgos físicos, como los inspeccionados por los mecanismos biométricos.

A continuación se describe un método de autenticación por cada tipo de reto.

2.1. Contraseñas

Las contraseñas responden al reto de identificar al individuo de acuerdo a "algo que el usuario conoce", que el sistema pueda verificar y que nadie más pueda adivinar[8]. las contraseñas, puede ser considerado el mecanismo más ampliamente usado y popular[8]; esto se debe a dos aspectos: costo y conveniencia. Por una parte se puede considerar que asignar una contraseña no tiene precio, como lo puede tener la expedición de una tarjeta inteligente o un token; de otra parte si se compromete una contraseña simplemente se reasigna una nueva; sin embargo ¿qué se debe hacer si se comprometen los datos biométricos de un usuario? [8].

Mark Stamp indica que este mecanismo tiene una deficiencia y es la elección de contraseñas adecuadas, los usuarios tienden a asignar contraseñas débiles[8], el usuario debe recordar las contraseñas por lo que tiende a utilizar palabras conocidas y representativas para él, pocas veces se utilizan contraseñas aleatorias que podrían considerarse más robustas pero difíciles de recordar. Una tercera opción en la selección de contraseñas es la utilización de frases codificadas "passphrases" que da la facilidad de recordarla para el usuario pero difícil de adivinarla por parte de un tercero. De acuerdo a experimentos realizados los mejores resultados a nivel de seguridad y recordación fueron obtenidos por parte de usuarios que escogieron una contraseña con el método de passphrases[8].

2.2. Tarjetas inteligentes (Smartcard)

Un ejemplo de mecanismos de autenticación basado en "algo que los individuos tienen" son las tarjetas inteligentes. Estas son un conjunto de dispositivos en forma de tarjeta que cuentan con un micro-chip para transmitir, almacenar o procesar datos[60]; estas capacidades les da el nombre de inteligentes. La Figura 4 presenta la clasificación de las tarjetas según Wolfgang Rankl[61].

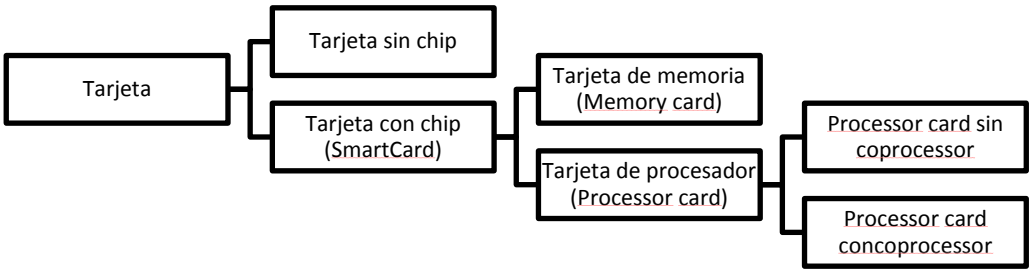

Figura 4. Clasificación de tarjetas, adaptado de [61]

La importancia de las tarjetas inteligentes en los procesos de autenticación está dada por sus capacidades que les permiten almacenar contraseñas, llaves simétricas, certificados digitales, imágenes biométricas, archivos de generación OTP (One Time Password), también les permiten generar pares de llaves asimétricas[62] y realizar cálculos y operaciones de seguridad.

2.3. Biométricos

Como representación de autenticación basada en "algo que el usuario es" podemos encontrar los mecanismos biométricos, estos son basados en características físicas o de comportamiento de los usuarios[63]; estas características deben cumplir con: ser universal, aplica sobre cualquier individuo; distinguible, diferencia con certeza un individuo de otros; permanente, no cambian en largos periodos de tiempo; obtenible, fácil de obtener sin daño al individuo; y finalmente ser confiable, robusto y de fácil de uso[8].

Los mecanismos de autenticación biométricos pueden utilizar dos tipos de credenciales[63]: credenciales estáticas, basados en un patrón estático calculado sobre una característica del usuario, como lo puede ser una huella digital o un patrón de retina. También se utilizan las credenciales dinámicas, basadas en el reconocimiento de patrones de comportamiento del

usuario como lo puede ser la escritura o la velocidad de tecleado. Algunos de los métodos de autenticación biométrica son:

- Huella dactilar: es el método de autenticación biométrica más utilizado[63], consiste en extraer el patrón siguiendo los siguientes pasos: se captura la imagen de la huella dactilar, se aplican varios algoritmos de procesamiento de imágenes, se identifican puntos característicos de la imagen y se extraen[8]; finalmente se comparan con el patrón obtenido con anterioridad verificando que los puntos clave coincidan.
- Geometría de la mano: este biométrico se basa en las dimensiones y proporciones de las manos y sus dedos[63]. La geometría de la mano es un mecanismo menos exacto que el de Huellas dactilares, pero es fácil y rápido de medir[8].
- Escaneo de Iris: Este método se basa en la singularidad del tejido alrededor de la pupila llamado iris. El proceso consiste en tomar una fotografía del iris en blanco y negro, la imagen es procesada y finalmente comparada con el patrón original mediante el método de distancia de Hamming[63].

Existen otros biométricos como lo son scan de retina, geometría de la cara, patrones de piel, patrones de voz y patrones de escritura[8]. Los métodos de autenticación biométrica explicados son mostrados en la Figura 5.

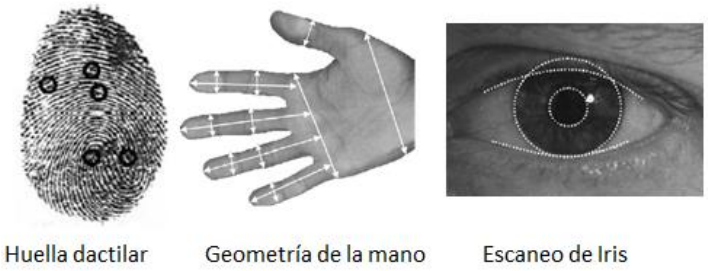

Figura 5. Métodos de autenticación biométricos[8]

2.4. Autenticación con cifrado de llave pública y certificados digitales

Dentro de las aplicaciones de la criptografía asimétrica se encuentra la autenticación, que es considerado un mecanismo muy robusto para este fin[63]. Las llaves asimétricas pública y privada explícitamente no representan una credencial, sin embargo dadas sus características pueden ser interpretadas de esta manera; la llave pública puede ser conocida por cualquier persona, de esta manera puede representar la identidad del usuario; por su parte la llave privada es secreta y de uso exclusivo del propietario, por esta razón puede ser tomada como una contraseña; finalmente el par de llaves están matemáticamente relacionadas lo que se asemeja al vínculo entre un usuario y su contraseña[63].

A continuación se presentaran algunos ejemplos de autenticación con llaves públicas en los cuales interactúa Alice (A) y Bob (B)[4], para este efecto se utiliza las siguientes notaciones:

- Mensaje (M)
- Cadena reto (R)
- Cifrado de mensaje con llave pública de Alice ($C = \{M\}_{Alice}$)
- Descifrado de C con llave privada de Alice ($M = [C]_{Alice}$)
- Firma de mensaje ($S = [M]_{Alice}$).

En el primer ejemplo Alice quiere autenticarse con Bob, el proceso consiste en que Bob cifra un mensaje reto con la llave pública de Alice, este mensaje solo se podrá descifrar con la llave privada de Alice, de esta manera si Bob recibe el mensaje original la autenticación es exitosa[8]. La autenticación puede realizarse también con firmas digitales, en este caso Bob enviará un mensaje a Alice, el cual será devuelto firmado digitalmente por Alice; La autenticación será exitosa si Bob puede verificar la firma digital del mensaje y comprobar que es el mensaje original. Para mejorar el rendimiento de cifrado en la conversación, es posible establecer en la autenticación una llave simétrica de sesión para este fin. La Figura 5 ejemplifica el proceso de autenticación con cifrado de llave pública y firma digital; en este ejemplo también se establece la llave de sesión entre Alice y Bob.

Figura 6. Llave de sesión y autenticación, adaptado de [8].

Finalmente, es posible establecer un protocolo de autenticación mutua o bidireccional; esto se logra utilizando en conjunto la llave privada del emisor y la llave pública del receptor para el intercambio del mensaje. Al igual que los ejemplos anteriores es posible realizar esta autenticación mediante cifrado de llave pública o firma digital, la **¡Error! No se encuentra el origen de la referencia.**Figura 7 ilustra los pasos de este tipo de autenticación.

Figura 7. Autenticación Mutua y llave de sesión, adaptado de [8].

[4] Ejemplos adaptados de [8] capítulo 9.

Como se presentó en los ejemplos anteriores la autenticación con criptografía asimétrica es muy robusta, sin embargo el uso de únicamente llaves presenta deficiencias por cuanto no se conoce otra información de las llaves en cuestión, como la fecha de generación, la fecha de caducidad, etc.[63]; bajo éste panorama suele utilizarse para autenticación mediante criptografía asimétrica, certificados digitales.

El certificado contiene meta data acerca del usuario e incluye su llave pública, así mismo se establece validez ya que es generado por un tercero confiable llamado Autoridad de Certificación (CA – Certificate Authority)[8]. El estándar X.509, el cual hace parte de la familia de estándares para la Infraestructura de Llave Pública (PKI)[64], definió la estructura y la semántica de los certificados y las listas de revocación de certificados (CRL),como también el proceso de validación mediante rutas de certificación[64].

La autenticación mediante certificados digitales fue utilizada en la solución S1581 del presente proyecto como mecanismo fuerte de autenticación. Se empleó tanto para autenticar usuarios como para autenticar servidores y clientes de Servicios Web.

2.5. Autenticación multi-factor

Cada una de las aristas explicadas anteriormente, "algo que el usuario conoce", "algo que el usuario tiene" o "algo que el usuario es", representa un factor de autenticación. El escenario más común es utilizar un único factor de autenticación o single-factor, por ejemplo empleando validación mediante contraseña[63]. Sin embargo para ciertas situaciones no es lo suficientemente robusto está aproximación, por lo que se requiere emplear varios factores; a esto se le conoce como un esquema de autenticación multi-factor[63].

Un ejemplo común es el del uso de un cajero electrónico, en el cual se requiere presentar la tarjeta débito (algo que el usuario tiene) y también se requiere digitar el PIN (algo que el usuario sabe); en este caso se utiliza una autenticación de dos factores. Si se utiliza mezcla de las 3 aristas: "algo que el usuario conoce", "algo que el usuario tiene" o "algo que el usuario es", se referenciara como una autenticación de triple factor[8].

La utilización de múltiples mecanismos de autenticación busca incrementar la seguridad del sistema haciendo que el riesgo residual del uso de un mecanismo sea mitigado con el uso de los otros factores; Esta estrategia requiere mayor inversión en dinero y tiempo del usuario para ser validado y acceder al recurso[63].

En la solución S1581 el concepto de autenticación de múltiple factor inspiró el desarrollo de diferentes mecanismos de autenticación de acuerdo al nivel de riesgo de la funcionalidad a acceder; dentro de la sección de arquitectura se explica este concepto bajo el título de "Autenticación multinivel".

2.6. OpenID

OpenId es una tecnologías de identidad abierta (*Open Identity*) centrada en el usuario "user-centric" o dirigidas por el usuario "user-driven", que permite a los usuarios registrarse e ingresar a múltiples sitios utilizando un mismo identificador[65]. OpenId permite descentralizar

la autenticación a un tercero llamado proveedor OpenID, con el cual los usuarios pueden gestionar una única cuenta. Entre los proveedores de servicios OpenID se encuentran AOL, Google, Yahoo, MyOpenID, entre otros[66].

Existen algunas tecnologías para delegación o federación de autenticación, como lo es SAML (*Security Assertion Markup Language*) que ha sido adoptado significativamente por la industria[67]; estas iniciativas por lo general requieren que las partes estén pre configuradas y que establezcan una relación de confianza previa para poder funcionar[65]. Sin embargo OpenID permite delegar la autenticación sin la necesidad de tener una relación de confianza preestablecida. OpenId se basa en intercambio de información cifrada mediante solicitudes http de un navegador web, entre el proveedor del servicio (*relying party*) y el proveedor de la identidad (*identity provider*)[66].

De acuerdo al *OpenID Foundation* algunas de las ventajas de utilizar este protocolo son: simplifica el ingreso a los sitios web, permite la portabilidad de la identidad, se utilizan las mismas credenciales para el ingreso de múltiples sitios y servicios, automatiza el intercambio de información, útil por ejemplo para el registro en un nuevo sitio[65]. De acuerdo al documento Open Trust Frameworks for Open Government[65], las tecnologías abiertas de identidad pueden apoyar significativamente en el desarrollo de políticas de *open government* y *e-goverment* ya que pueden agilizar y simplificar las soluciones de identidad digital de los ciudadanos[65][68].

Dadas las características del protocolo OpenID, en este proyecto se ha tenido en cuenta para desarrollar los componentes de autenticación dirigidos al ciudadano.

3. Autenticación e identificación del ciudadano y soluciones de gestión de datos personales.

En el ámbito del gobierno electrónico existe un creciente desarrollo de los países en el uso de tecnología para el apoyo de sus políticas, esto permite incrementar la eficacia, transparencia, capacidad de respuesta, la participación e inclusión en la prestación de servicios públicos[69]. De acuerdo a la encuesta 2012 sobre E-Government de las Naciones Unidas, los gobiernos están pasando de modelos de organización descentralizados a modelos que pretenden centralizar en un portal único todos los servicios prestados al ciudadano[69]. Estas tendencias traen retos significativos en temas de seguridad, principalmente en identificación y autenticación de los ciudadanos. A continuación se presentan algunos avances realizados sobre tecnologías y servicios de autenticación y consulta de datos personales por parte del ciudadano.

Existe un esfuerzo importante de algunos países en convertir los documentos de identidad en un mecanismo para acceso a servicios, en especial en la Unión Europea se ha desarrollado este concepto como documento de identidad electrónico (DNIe)[70], El Estudio sobre Mejores Prácticas en Gobierno Electrónico en Europa, realizado por el Ministerio Español de Política Territorial y Administración y Capgemini Consulting[70], indica que la Identificación Electrónica (eID) "*es la clave para combinar la apertura y flexibilidad con una adecuada protección de la intimidad y una mayor seguridad en los entornos electrónicos*"[70]. La Tabla 1 lista algunos países que han desarrollado documentos de identificación electrónica.

País	**Iniciativa de e-identificación**
Estonia	**MobileID**: Sistema de identificación electrónica basado en tarjetas y firma digital.
Austria	**e-Signature**: Tarjeta del Ciudadano (Bürgerkarte)
Suecia	**SteriaID:** Acceso a servicios de administración electrónica **BankID:** Identificación electrónica en Suecia, basada en PKI (Public Key Infrastructure)
Italia	**PEC:** *Posta Elettronica Certificata*
Alemania	*Elektronischer Personalausweis*
Bélgica	**eID:** *Carte d'identité électronique*
España	**DNIe:** Documento Nacional de Identidad electrónico
Rumania	**Documento de identidad electrónico**
Perú	**DNI electrónico**
Brazil	**RIC:** *Registro de Identidade Civil*
Argentina, Bolivia, Cuba, Venezuela (Próximamente)	**DNI electrónico**
Portugal, Lituania, Finlandia, Portugal	**e-ID**

Tabla 1. Países vs Iniciativas de documento de identidad electrónico, adaptado de [70][71][72][73][74][75].

Bélgica es uno de los países que primero incursionó en la aplicación de tarjetas de identificación electrónica en el año 2000, la tarjeta de Identificación eID, cuenta con dos certificados digitales, enfocados a tareas de autenticación y de firma digital, se puede utilizar para acceso a servicios online y presentación electrónica de documentos oficiales[70]. En el sitio central belgium.be se unifican servicios que pueden ser accedidos de manera electrónica; este sitio tiene la particularidad de tener, dependiendo del tipo de servicio al que se requiera acceder, cuatro niveles de autenticación, así: 1, no requiere contraseña; 2, requiere contraseña; 3, requiere contraseña y token; 4, requiere identificación electrónica.

En los países bajos existe DigiD (Identificación Digital), que permite a los ciudadanos y empresas acceder a servicio en línea, cuenta también con varios niveles de autenticación así: bajo, usuario y contraseña; medio, autenticación sms; Alto, Enik (e-ID) – PKI. La iniciativa para acceso a los servicios por parte de los ciudadanos es llamada "Personal DigiD"[70]. Estonia por su parte cuenta con MobileID, el cual permite mediante la tarjeta SIM del celular realizar procesos de autenticación y firma electrónica de documentos.

El enfoque de autenticación por niveles ha influenciado significativamente este trabajo y se ha tenido en cuenta para la generación de los mecanismos de autenticación de la solución S1581(Ver Capitulo IV - 3.2 Descripción de la arquitectura).

De otra parte, algunos países han desarrollado como respuesta a la política de "Mejora de la Transparencia" soluciones basadas en tecnología para permitir a los ciudadanos localizar sus datos personales, saber quien accedió a ellos y con qué fin; este es el caso de Dinamarca con MyPage(https://www.borger.dk)[76], esta solución permite acceder a información de impuestos, vivienda o datos del registro civil. Mon Dossier (http://www.belgium.be)[77] solu-

ción Belga permite a los ciudadanos "*comprobar y rectificar su información personal online en el Registro Nacional de Bélgica. También permite a los usuarios conocer quién ha accedido a su información personal*"[70]. Finalmente, para consultar o modificar los datos personales tratados por las entidades públicas, Holanda cuenta con la solución Mi Gobierno (https://mijn.overheid.nl)[78].

4. Tecnologías de desarrollo web

A continuación se explica brevemente las tecnologías de desarrollo web que influenciaron o fueron aplicadas en este proyecto.

4.1. Java Platform, Enterprise Edition (Java EE)

Java Platform, Enterprise Edition (Java EE) es una plataforma estándar para el desarrollo de aplicaciones empresariales[79]. Java EE comprende un conjunto de especificaciones que se cimienta sobre *Java Platform, Standard Edition*(Java SE) para el desarrollo de aplicaciones distribuidas, transaccionales, portables y orientadas a ejecución en ambientes de alta disponibilidad[5][80].

Sun Microsystems desarrollo inicialmente la plataforma en 1999 bajo el nombre J2EE 1.2, la cual se fue complementando con las versiones 1.3 y 1.4 ; J2EE fue señalado de ser un modelo de componentes complejo y difícil de probar, implementar y ejecutar[80]. En 2006 la plataforma se convierte en Java EE (JEE); esta versión incluyó elementos de iniciativas abiertas que la hicieron más flexible que su antecesor[80]. La versión inicial de Java EE fue la 5, y la más reciente es la 7. Este trabajo de grado fue desarrollado con Java EE 6 (JEE6) ya que es la distribución vigente para ambientes de producción. Las principales características de JEE son[5][79][80]:

- Gestión de la capa de presentación mediante Servlets, JavaServer Pages (JSP) y Java Server Faces (JSF).
- Soporte a la capa de negocio mediante componentes Enterprise Java Beans, colas de mensajes Java Message Service, transacciones con Java Transaction API, solicitudes asíncronas , "*timer service*, y RMI/IIOP.
- Servicios web SOAP y RESTful.
- Manejo de persistencia con Java Persistence API (JPA)
- Flexibilidad de desarrollo con el uso de Anotaciones, Injection, validación de Beanes, entre otras.

4.2. Servicios web

Los servicios web (web services) son una forma estándar de conectar diferentes piezas de software bajo diferentes plataformas, lenguajes y *framewoks*, permitiendo así su interoperabilidad[5]. El principio de estos servicios es el de encapsular la lógica de negocio y exponer una interfaz que pueda ser invocada fácilmente desde un cliente.

Los servicios web inicialmente se basaron en el uso del lenguaje XML para lograr compatibilidad entre plataforma heterogéneas, así surgieron los Servicios Web SOAP (*Simple Object Access Protocol*)[5]. SOAP plantea el intercambio de mensajes de solicitud respuesta utilizando estructuras XML definidas[80]. Estos servicios requieren ser definidos de manera formal mediante el descriptor llamado WSDL(*Web Services Description Language*)[81] el cual indica el formato y arquitectura del mensaje. SOAP se caracteriza por ser independiente del protocolo de comunicación, aunque son comúnmente utilizados sobre el protocolo HTTP[5]. Esta clase de servicios tiene una amplia trayectoria y han ganado una amplia adopción[5].

Por otra parte ha surgido *REpresentational State Transfer* (REST), un estilo de arquitectura que permite la definición de servicios web de manera más sencilla al tradicional Servicio web basado en SOAP[82]. Su facilidad de uso ha permitido que se posicione como el modelo predominante de Servicios Web[82]. RESTful es auto descrito[83] y no requiere de archivos descriptores adicionales como el wsdl para SOAP, se enfoca en acceder a los recursos mediante métodos http a través de UR's (*Universal Resource Locator*)[81]. Otra ventaja de REST es el bajo consumo de recursos, esto lo convierte en el candidato ideal para dispositivos móviles[81].

Aunque RESTful presenta varias ventajas sobre los servicios basados en SOAP, tiene una debilidad respecto al manejo de seguridad ya que no cuenta con un modelo especifico en este ámbito[83]. La ausencia de metadata en RESTful limita el uso de mecanismos de seguridad; la seguridad se restringe a la proporcionada por la capa de transporte o la realizada de manera ad-hoc por el desarrollador[83]. En el ámbito de seguridad los servicios basados en SOAP cuentan con la especificación WS-Security (WSS)[67] el cual busca principalmente mantener la integridad y confidencialidad del mensaje SOAP. WS-Security es un modelo abstracto de seguridad que utiliza tokens de seguridad en conjunto con firmas digitales para proteger y autenticar los mensajes SOAP[84].

4.3. Framewoks de desarrollo

El framewok de desarrollo es la plataforma que permite la construcción ágil y robusta de una aplicación. Para la solución S1581 se evaluaron 2 frameworks provistos por la comunidad JBoss, los cuales tiene un alto nivel de utilización en el desarrollo de proyectos empresariales. Estos framework son: Seam 2.2[85] y JBoss Developer Framewok (jdf) 2.1[86].

Seam 2.2 es un framewok que proporciona un conjunto de herramientas para desarrollo sobre plataforma JavaTM 2 Platform Enterprise Edition, v 5.0 (JEE5)[85]. Seam es una plataforma robusta, ampliamente utilizada y cuenta con amplia documentación; a pesar de esto el proyecto fue cancelado debido a que varias de sus funcionalidades fueron integradas a JEE6[87].

Por su parte JBoss Developer Framewok (jdf) es una nueva plataforma que permite crear aplicaciones utilizando un gran conjunto de tecnologías JBoss[86]. Esta plataforma soporta JEE6, EJB 3.1, JPA2, JSF2 y un conjunto de nuevos estándares y tecnologías[86]. Jdf cuenta con la herramienta JBoss Forge[88], la cual permite automatizar y optimizar tareas como las de generación de código, configuración de la aplicación, despliegue de la aplicación, entre otras.

4.4. Servidor de aplicaciones

Para que una aplicación JEE pueda ejecutarse requiere de un entorno de ejecución denominado contenedor de aplicaciones. Los contenedores brindan a la aplicación servicios transaccionales, de gestión de recursos, de seguridad, de acceso a bases de datos, entre otros[80]. Diferentes fabricantes han implementado sus contenedores o servidores de aplicación; algunos de los más destacados son: JBoss Application Server[11], Oracle WebLogic Server[89] e IBM WebSphere Application Server[90].

En el desarrollo de este proyecto se utilizó JBoss Application Server 7.1 (JBoss AS 7.1) [11] como servidor de aplicaciones. Se resalta la importancia de este componente de infraestructura ya que para poder acceder apropiadamente a servicios como autenticación con certificados digitales, uso de cifrado mediante https, dominios de seguridad, *pooles* de conexión a Bases de datos, entre otros, se requiere realizar exigentes procesos de configuración que son específicos para el contenedor utilizado.

4.5. JSON

JavaScript Object Notation - Notación de Objetos de JavaScript (JSON)[7] es un formato de intercambio de datos ligero, que se caracteriza por ser fácil de entender y procesar. Esta notación está basada en el lenguaje JavaScript y es considerado independiente del lenguaje por ser basado en formato de texto[7]. Este lenguaje plantea que las estructuras de datos sean representada por una colección de parejas nombre, valor; un valor puede representar un arreglo de objetos u otra estructura de datos[7]. Por ejemplo, los atributos nombre y apellido del sujeto Carlos Camargo puede ser representado en notación JSON como *{"nombre":"Carlos", "apellido":"Camargo"}* (ver [7]). En este proyecto se utiliza esta notación para el intercambio de estructuras de datos en los servicios web (ver página 46).

La sintaxis de la estructura de los datos en JSON es auto contenida; sin embargo en ciertos casos se requiere describir o especificar los mensajes JSON. *JSON Schema* permite representar dicha estructura en un lenguaje sencillo a través de metadatos[91]. En este proyecto se utiliza JSON Schema para la especificación de integraciones.

5. Metodologías ágiles e historias de usuario

En el año 2001 se generó el manifiesto “Manifiesto para el Desarrollo Ágil de Software”[92] el cual presenta una seria de principios a ser aplicados para optimizar el proceso de desarrollo tradicional. Esta declaración Ágil resalta elementos tales como “Individuos e interacciones”, “Software funcionando”, “Colaboración con el cliente”, “Respuesta ante el cambio” [92]. El manifiesto tiene en cuenta experiencias de autores como Kent Beck, Ron Jeffries, Jeff Sutherland, entre otros; estos autores desarrollaron metodologías como Scrum[93] y *eXtreme Programming* (XP)[20], las cuales son consideradas como “ágiles”.

Scrum, creado en 1993 por Jeff Sutherland[94], se considera un proceso o metodología de gestión de proyectos ágil[93] que puede ser aplicada a cualquier tipo de proyecto, aunque es más comúnmente utilizada en proyectos de desarrollo de software[94]. Scrum puede ser

utilizado en proyectos que cambian rápidamente o en proyectos en los cuales los requerimientos surgen o pueden ser modificados con frecuencia[93]. El planteamiento de esta metodología es tener iteraciones cortas, entre una y cuatro semanas, llamadas *sprints*; el objetivo de cada sprint es entregar una porción del desarrollo totalmente funcional[94].

Extreme Programming(XP) por su parte es una metodología de desarrollo ágil de software, planteada por Kent Beck en 1996[19]; al igual que scrum, XP permite adaptarse a los requerimientos cambiantes de los proyectos. XP contempla 5 valores como elementos de mejora dentro de los proyectos, estos son: simplicidad, comunicación, retroalimentación, coraje, y respeto[20]. Esta metodología permite tener ciclos de desarrollo corto, retroalimentación temprana, continua y concreta, una visión de planeación incremental, flexibilidad en los tiempos de implementación de funcionalidades para responder a las necesidades de negocio, mayor comunicación entre el equipo de trabajo, el cliente y los patrocinadores, entre otros[19].

En las metodologías agiles se utiliza el concepto de historias de usuario para la identificación y gestión de requerimientos. Una historia de usuario describe una funcionalidad que será de gran valor para el usuario final o patrocinador del proyecto[21]; pretende ser una descripción simple, clara y corta de la funcionalidad[21]. De acuerdo a Mike Cohn [21], cada historia se compone de tres elementos: una descripción, que corresponde a un texto escrito de manera sencilla en términos del usuario; conversaciones definidas como interacciones entre el usuario y el equipo de trabajo para profundizar en los detalles de la historia; y finalmente pruebas de aceptación que permiten definir los parámetros bajo los cuales se considera que una Historia de Usuario ha sido desarrollada completamente.

Bill Wake[95] plantea que las historias de usuario deben orientarse bajo los principios *INVEST*:

- **Independiente:** Una historia de usuario no debe depender de otra historia ya que esto facilitará la priorización de las mismas.
- **Negociable:** Las historias de usuario no deben ser la base contractual del proyecto, deben ser flexibles y pueden cambiar y evolucionar a lo largo de la ejecución del proyecto, incluso podría dejar de tenerse en cuenta si así el cliente lo desea.
- **Valiosa:** La historia de usuario debe brindar valor al proyecto y al usuario final.
- **Estimable:** Cada historia de usuario debe poder ser medida en términos del tiempo que tomará en implementarse.
- **Pequeña:** La historia de usuario debe ser pequeña y concisa. Si una historia de usuario es muy grande ésta se debe dividir en otras historias más pequeñas.
- **Verificable:** la historia de usuario debe poderse probar en un proceso de calidad.

Las metodologías agiles, en particular *Extreme Programming (XP),* y las Historias de Usuario fueron tenidas en cuenta en la metodología utilizada para el desarrollo del presente proyecto.

IV - DESARROLLO DEL PROYECTO

En este capítulo se presenta las definiciones, artefactos y actividades relevantes realizadas en la ejecución del proyecto, así como las características principales de la Solución Informática S1581.

1. Taxonomía de datos personales

Para dar cumplimiento a la ley las entidades en primera instancia debe realizar un análisis cuidadoso de qué datos personales gestionan. Esta es una tarea difícil por cuanto la ley describe el significado de dato personal pero no dice nada de cuales son y mucho menos acerca de las principales clasificaciones que pueden existir. Como guía para la implementación de la solución S1581 se ha realizado un avance inicial en la definición de una taxonomía de datos personales cuyo fin es establecer las categorías principales y la identificación de los datos más comunes.

Para la realización de esta taxonomía se han tenido en cuenta los tipos de datos personales plasmados en la ley colombiana de protección de datos[3], la directiva europea 95/46/CE[32], las clasificaciones que algunas entidades han realizado de los datos personales como el "sistema personas" a cargo del "Instituto Federal de Acceso a la Información y Protección de Datos" (IFAI)[96], Agencia Española de Protección de Datos[97] y aporte propio del autor.

La taxonomía propuesta hace referencia a una estructura jerárquica que tiene como nodo principal la clasificación "dato personal", que actúa como raíz para agrupar las demás categorías. En el nivel 1, de acuerdo a las características comunes o interrelaciones de los datos personales, se establece grandes subdivisiones llamadas "*CLASES*". El nivel 2 consiste de FAMILIAS de datos que están muy relacionados o que hacen parte de un área común. En la taxonomía propuesta se establece un tercer nivel llamado "PARTICION" que es opcional y se deja abierto para que quien la utilice, pueda subclasificar de acuerdo a su criterio, el área de aplicación o al sistema específico. En caso de requerirse en la clasificación nuevos niveles, se podrá integrar bajo el mismo concepto aplicado a las "PARTICIONES". A continuación se describe a nivel general las CLASES de la taxonomía propuesta.

1. Datos biográficos: clasifican los datos referentes los hechos relevantes de la historia e identificación de una persona. Las subcategorías asociadas son: datos de identificación, datos académicos, datos laborales, reconocimientos y datos de origen.
2. Datos genéticos: hacen referencia a datos relacionados con las características biológicas de las personas, algunas sub clasificaciones son: características físicas, características Personales, datos biométricos.
3. Datos financieros: relaciona la información referente a las condiciones económicas y financieras del individuo. Generalmente se agrupan bajo el concepto de patrimonio el cual incluye información como ingresos, egresos, transacciones financieras, créditos, etc.
4. Datos de conducta: permite clasificar los datos enfocados a conocer el comportamiento de una persona. En esta clase se encuentran relacionados los hábitos, gustos y aficiones, datos legales, datos ideológicos, vida sexual, etc.

5. Datos de relaciones humanas: mediante esta clase es posible catalogar la información sobre la relación del individuo y otras personas. Por ejemplo de filiación entre un padre e hijo, lazos de amistad, referencias personales, etc.
6. Datos de contexto: mediante esta categoría se puede agrupar los datos de elementos externos que influyen sobre la persona o la relacionan al mundo. Por ejemplo bajo esta clase se clasificaría la información recolectada por sensores tales como GPS.
7. Datos de salud: se agrupan los datos referentes al bienestar físico o mental del individuo. Las enfermedades e historias clínicas son clasificadas en esta clase. Los datos de salud son de particular cuidado ya que son considerados sensibles; es la única clase que a nivel global tiene este estatus y por tanto implica que los datos requieren especial atención en su gestión.

La Tabla 2 muestra las CLASES y FAMILIAS provistas en la taxonomía de datos personales de la solución S1581, se marcan con asterisco (*) las clasificaciones que son consideradas sensibles.

CLASE	**FAMILIA**
Datos biográficos	Datos de identificación
	Datos académicos
	Datos laborales
	Reconocimientos
	Datos de origen *
Datos genéticos	Características físicas
	Características personales
	Datos biométricos.
Datos financieros	Datos patrimoniales
Datos de conducta	Hábitos
	Gustos y aficiones
	Datos legales
	Tránsito y movimientos migratorios
	Datos Ideológicos *
	Vida sexual *
Relaciones Humanas	Familiares
	Amistades
Datos de contexto	Contexto
Datos de salud	Datos de Salud *

Tabla 2. Taxonomía de datos personales S1581

En la sección de anexos se puede encontrar un conjunto de datos de uso común, el cual ha sido organizado de acuerdo a la taxonomía propuesta en este trabajo; este documento puede ser utilizado como orientación para las empresas que requieran hacer el proceso de clasificación de la información personal.

La Tabla 3 muestra a manera de ejemplo la clasificación para 3 datos personales: nombre, peso, y cupo disponible para una tarjeta de crédito; en la muestra, nombre es un dato de tipo identificación dentro de datos biográficos, para nombre y peso es suficiente la clasificación de CLASE y FAMILIA. Sin embargo, para "cupo disponible" se sugiere tener un tercer nivel que indica el tipo de producto de crédito al que se está haciendo referencia.

DATO PERSONAL	Nombre	Peso	Cupo disponible
CLASE	Datos biográficos	Datos genéticos	Datos financieros
FAMILIA	Datos de identificación	Características Físicas	Historial crediticio
PARTICION	n/a	n/a	Tarjetas de crédito

Tabla 3. Ejemplos de clasificación de datos personales

La importancia de esta taxonomía para la solución S1581, radica en la generación de un lenguaje común que permitió desarrollar módulos especiales de presentación y búsqueda de la información.

2. Funcionalidades de la solución informática S1581

En esta sección se explicarán los requerimientos que guiaron el desarrollo del proyecto y las funcionalidades que finalmente se implementaron en la solución informática S1581.

De acuerdo a las metodologías Agiles Scrum y *Extreme Programming (XP)*, se ha seleccionado el concepto de Historias de Usuario para documentar los requerimientos del proyecto (ver explicación de estos conceptos en la sección 5 del marco teórico). En este proyecto las historias de usuario se han obtenido del análisis de la ley Colombiana de protección de datos[3][4], de las leyes internacionales como LOPD[12] y los esfuerzos que realizan entidades nacionales e internacionales como la Superintendencia de Industria y Comercio[98] y la Agencia Española de Protección de Datos Personales[99].

A continuación se describen los actores identificados, el proceso realizado para la definición de funcionalidades y las historias de usuario que fueron implementadas en la solución.

2.1. Actores

Se han identificado tres actores principales de la solución: el ciudadano, las entidades y la Superintendencia de Industria y Comercio.

- **Ciudadano colombiano**: se considerara ciudadano, al natural de Colombia, colombiano, que haya adquirido la ciudadanía; de acuerdo a la constitución "la ciudadanía se ejercerá a partir de los dieciocho años" [2]. La solución s1581 facilita a los ciudadanos ejercer los derechos establecidos en la ley 1581 de 2012, la consulta para menores de edad no está contemplada.
- **Entidad**: Persona Jurídica que pueda ser considerada responsable o encargada del tratamiento de datos personales[3]. La solución S1581 interactuará con sistemas o

plataformas tecnológicas de las entidades, que contengan información personal y que hayan sido integradas a la solución. Se da acceso a las entidades a algunas funcionalidades que permiten conocer el estado y estadísticas del servicio prestado[5].

- **Superintendencia de Industria y Comercio**: Autoridad en materia de protección de datos personales, mediante la "Delegatura para la Protección de Datos Personales"[3, p. 15], vigila el cumplimiento de la Ley 1581 de 2012. La solución s1581 expone algunas funcionalidades que pueden apoyar la labor de esta entidad.

2.2. Historias de Usuario

En este proyecto para detallar las funcionalidades y crear las historias de usuario se analizaron los documentos referentes a la Ley de protección de datos (Ley 1581 de 2012, proyecto de decreto[6], decreto 1377 de 2013, sentencia C748/11) y se han realizado reuniones con funcionarios de la Superintendencia de Industria y Comercio[7]. En el análisis se identificaron 30 Historias de Usuario que potencialmente podrían incluirse en la solución informática S1581; En el inventario realizado se incluyó para cada Historia de Usuario la siguiente información:

- **ID Historia**: presenta el identificador asociado a la Historia de Usuario.
- **Fuente**: indica el elemento que fue analizado para dar origen a la Historia de usuario.
- **Descripción fuente**: contiene una referencia al texto de la norma o de la fuente.
- **Funcionalidad** – Historia de Usuario: se describe la historia de usuario.
- **Justificación**: Elementos tenidos en cuenta para hacerla candidata a ser parte de la solución.
- **Clasificación FURSP+**: Indica la clasificación dada a la Historia de usuario bajo los tipos de requerimientos: *Funcionality (*Funcionalidad*), Usability (*Usabilidad*), Reliability (*Confiabilidad*), Performance (*Rendimiento*), Supportability (*Soporte*), Others (*Otros*)*[100].
- **Actor**: Indica el actor al que está enfocada la funcionalidad.
- **Nivel de riesgo**: Para cada Historia de Usuario se asignó una valoración de riesgo de acuerdo al tipo de dato involucrado u operación que se realiza. Se utilizó una escala de niveles de riesgo de 1 a 3, en la cual 1 indica un nivel bajo, 2 nivel de medio y 3 un nivel alto.

[5] Aunque la ley contempla como responsables y encargados a personas naturales, estas no se tendrán en cuenta en este trabajo, sin embargo si llegara a cumplir los requisitos tecnológicos podría hacer uso de la solución S1581.

[6] En el momento de identificar las funcionalidades, aun no se había publicado el decreto 1377 de 2013, por lo que se tomó como base la propuesta de proyecto para algunas Historias de Usuario. Con la salida del decreto se incluyeron algunas otras funcionalidades.

[7] Reuniones realizadas en el mes de marzo de 2013 con Carlos Enrique Salazar Muñoz, Director de investigación de protección de datos personales y Aida Lucia Hurtado Bejarano Ingeniera de esta misma unidad.

En la Tabla 4 se presenta, a manera de muestra, la documentación generada para la Historia de Usuario con código H1. En el anexo 2 se encuentra la documentación para todas las Historias de Usuario identificadas.

ID Hist	H1
Fuente[8]	Ley 1581-12, Artículo 1°: " La presente ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos".
Historia de Usuario / Funcionalidad	Un ciudadano puede consultar el nombre las entidades que almacenan sus datos personales.
Justificación	Como ciudadano se puede tener nociones de algunos lugares en donde están registrados sus datos personales; sin embargo, no se conoce la totalidad de entidades que pueden tener acceso a dicha información. Esta funcionalidad permitirá sobrepasar la barrera del desconocimiento, habilitando al ciudadano en la identificación de las entidades en donde están sus datos personales. Facilitará la facultad de "conocer" la información recogida acerca de las personas establecida en el derecho hábeas data[1][11]. Se considera que esta es una de las funcionalidades principales de la solución S1581.
Clasif. FURPS	F (Funcionalidad)
Actor	C. (Ciudadano)
Nivel de riesgo	1 (Riesgo Bajo)

Tabla 4. Ejemplo de documentación de Historia de Usuario

2.3. Selección de funcionalidades

En el proyecto se utiliza la metodología de Análisis y Resolución de decisiones (DAR)[101], con el cual se buscó establecer las funcionalidades a implementar de la Solución S1581, teniendo en cuenta las demandas de la ley 1581, las necesidades de los ciudadanos, los lineamientos de la Superintendencia de Industria y Comercio, y los tiempos y alcances establecidos para el desarrollo de este proyecto de grado.

[8] En el anexo 2 se encuentra la descripción detallada de cada fuente donde se obtuvieron las Historias de Usuario.

Para realizar el análisis DAR se ha definido como alternativas cada una de las funcionalidades plasmadas como Historias de Usuario. De acuerdo al proceso DAR, se realizó una evaluación de costo y tiempo de las alternativas, de igual manera se realizó el proceso de cálculo de un índice de calidad y de adecuación a las necesidades. A continuación se describe estos pasos.

2.3.1. Evaluación de costo y tiempo de las alternativas

Para cada alternativa se asocia el costo y tiempo estimado para su realización. El tiempo refleja la complejidad que puede significar cada Historia de Usuario; las actividades para realizar historias con complejidad alta tiene asociado entre 10 y 12 días de desarrollo, por su parte las historias de usuario con complejidad media se les asocia una duración de 5 días, finalmente para actividades con complejidad baja se asocian una duración de 3 días.

2.3.2. Cálculo de índice de calidad y de adecuación a las necesidades

El cálculo del índice de calidad en el contexto de este proyecto se realizó teniendo en cuenta 2 criterios globales: pertinencia y utilidad, a cada uno de ellos se asignó un peso en la evaluación de 50%. A continuación se describe cada criterio global y sus criterios específicos.

1. **Pertinencia:** Este criterio permite identificar si una funcionalidad a implementar en la solución informática S1581 es conveniente, oportuna y adecuada en el ámbito de protección de datos personales en el contexto colombiano. Los siguientes son los criterios específicos tenidos en cuenta:

   - Apoyo al ciudadano: La funcionalidad ayuda a los ciudadanos para hacer cumplir sus derechos en materia de protección de datos personales.
   - Coherencia con la ley: Soporta, complementa, o permite la aplicación de la ley 1581 de 2012.
   - Afinidad con políticas y procesos: La funcionalidad es afín a las políticas o procesos que se están desarrollando en materia de protección de datos personales, tanto en el ámbito público como el privado.
   - Compatibilidad tecnológica: La funcionalidad es coherente y está alineada con otros proyectos que se están desarrollando en materia de protección de datos personales, particularmente con los que son apoyados por TIC's.

2. **Utilidad:** Este criterio permite identificar si la funcionalidad produce un beneficio para el ciudadano. Los siguientes son los criterios específicos tenidos en cuenta:

   - Beneficio: El uso de tecnología para implementar la funcionalidad presenta beneficios tangibles al ciudadano.
   - Simplificación de trámites: Facilita al ciudadano la gestión de sus datos personales. Se tiene en cuenta elementos como reducción de pasos, tiempo o desplazamiento para realizar una actividad.

- Relevancia: Identifica si la funcionalidad es importante o representativa para la gestión de datos personales.

La Tabla 5 presenta la asignación de pesos tenida en cuenta en la evaluación de funcionalidades mediante el método DAR, para cada criterio global y específico. Cada alternativa se evaluó en una escala entre 1 y 5, siendo 1 un valor que representa poco significativo y 5 representa muy significativo.

1. Pertinencia			**50%**	**2. Utilidad**	**50%**	
Apoyo al ciudadano	**Coherencia con la ley**	**Afinidad políticas y procesos**	**Compatibilidad tecnología**	**Beneficio**	**Simplificación de trámites**	**Relevancia**
25%	25%	25%	25%	30%	30%	40%

Tabla 5. Pesos de evaluación de criterios globales y específicos

El proceso de selección se realizó mediante reuniones con funcionarios de la Director de investigación de protección de datos personales de la SIC[9], a quienes se les presentaron las funcionalidades y dieron su opinión y valoración de las funcionalidades. De otra parte se tuvo en cuenta el criterio técnico del autor del trabajo de grado. Las funcionalidades seleccionadas para ser implementadas son las que obtuvieron un valor entre 4 y 5. La Tabla 6 presenta las 17 funcionalidades implementadas en la Solución Informática S1581(ver calificación en **¡Error! No se encuentra el origen de la referencia.**).

ID Hist.	**Historia de Usuario**
H1	Un ciudadano puede consultar el nombre las entidades que almacenan sus datos personales.
H2	Un ciudadano puede consultar los datos personales que tiene registrada una entidad acerca de él.
H3	Un ciudadano puede consultar los datos sensibles que tiene registrada una entidad acerca de él.
H4	Un ciudadano puede solicitar la rectificación de sus datos personales.
H5	Un ciudadano puede consultar la autorización dada a una entidad para el tratamiento de sus datos personales.
H6	Un ciudadano puede consultar la autorización otorgada a una entidad para el tratamiento de sus datos sensibles.
H7	Un ciudadano puede consultar la finalidad del tratamiento de sus datos personales por parte de una entidad.

[9] Reuniones realizadas en el mes de julio de 2013 con Carlos Enrique Salazar Muñoz, Director de investigación de protección de datos personales y Aida Lucia Hurtado Bejarano Ingeniera de esta misma unidad.

H9	El ciudadano puede consultar el aviso de privacidad de la entidad, en el cual se incluye las políticas de tratamiento de su información, la forma de acceder a las mismas y las características del tratamiento.
H10	El ciudadano puede solicitar a la entidad rectificación de sus datos personales. Esta solicitud es enviada mediante correo electrónico a la entidad involucrada.
H11	El ciudadano puede solicitar a la entidad la revocación de la autorización de tratamiento de datos. Esta revocación abarca todos los usos y finalidades. Esta solicitud es enviada mediante correo electrónico.
H21	La solución informática debe contar con un mecanismo de control de acceso adecuado que garantice que solo el titular tendrá acceso a su información personal.
H23	El sistema lleva un registro de ingreso a la solución, consultas realizadas a las entidades y solicitudes de rectificación de información y revocación de autorización.
H25	Una entidad puede consultar las consultas y solicitudes que le han realizado en un periodo de tiempo.
H26	Una entidad puede consultar las consultas y solicitudes que le ha realizado un ciudadano.
H27	La Superintendencia de Industria y Comercio (SIC) puede consultar las consultas y solicitudes que se han realizado en todo el sistema en un periodo de tiempo.
H28	La SIC puede consultar las consultas y solicitudes que ha realizado un ciudadano.
H29	El ciudadano puede consultar los accesos, consultas y solicitudes que ha realizado en el sistema.

Tabla 6. Historias de Usuario implementadas en la solución informática S1581

3. Diseño de la solución informática S1581

En este capítulo se describe la arquitectura, los componentes, interfaces y elementos técnicos considerados para la Solución Informática S1581. Es importante resaltar que el diseño ha considerado elementos de seguridad y privacidad, tales como los mecanismos de autenticación del ciudadano y la seguridad entre los diferentes componentes de la solución; estos elementos también son expuestos en este capítulo.

3.1. Autenticación

Como se explicó en el marco teórico existen varios mecanismos de autenticación; algunos son sencillos, más fáciles de utilizar para los ciudadanos, y otros más complejos pero brindan mayor seguridad. Para establecer el mecanismo de autenticación adecuado se clasificaron el conjunto de todas las funcionalidades de acuerdo al nivel de riesgo; para este fin se definieron las siguientes categorías:

- **Riesgo medio**: Asociado a funcionalidades que permiten conocer la ubicación y responsables de los datos personales, pero no el detalle específico del valor de los datos. También se clasifican funcionalidades asociadas a reportes. Las Historias de usuario de esta categoría son: H1, H7, H16, H19, H26, H27, H28, H29, H30. (ver detalle de Historias de usuario en Anexo 1)

- **Riesgo moderado:** Asociado a funcionalidades que exponen información específica del ciudadano. Por ejemplo consultar la información personal que tiene registrada una entidad acerca de él. Las Historias de Usuario de esta categoría son: H2, H4, H8, H10, H11, H17, H20, H23. (ver detalle de Historias de usuario en Anexo 1)
- **Riesgo alto:** Asociado a funcionalidades que involucran modificaciones, acciones o solicitudes que el ciudadano realiza ante un tercero. Por ejemplo la solicitud de rectificación de datos ante una entidad. Las Historias de usuario de esta categoría son: H3, H5, H6, H9, H12, H13, H14, H15, H18, H21. (ver detalle de Historias de usuario en Anexo 1)

Dado que el componente de autenticación es el eje fundamental de seguridad de la solución S1581 fue necesario establecer una implementación híbrida que permita cumplir con la sencillez esperada por los ciudadanos y la seguridad que la ley y las entidades promueven y esperan. Esta implementación consiste en establecer niveles de autenticación los cuales serán utilizados en momentos y funcionalidades diferentes. Para esta definición se han tenido en cuenta las experiencias y enfoques presentados en el marco teórico en las secciones 2. Control de acceso y mecanismos de autenticación y 3. "Autenticación e identificación del ciudadano y soluciones de gestión de datos personales." Se estableció inicialmente la creación de 2 niveles, teniendo en cuenta que algunos mecanismos de autenticación pueden suplir las necesidades de seguridad para riesgos de nivel moderado y alto. Sin embargo, no se descarta a futuro incluir un tercer nivel que permita acceder a funcionalidades críticas o restringidas.

La solución s1581 provee un **servicio de autenticación nivel 1** que aplica de manera general al ingreso a la plataforma y a las funcionalidades que tienen un nivel de riesgo medio. De otra parte el **nivel 2 de autenticación** es utilizado para las funcionalidades que tengan riesgo moderado o alto; la solución S1581 provee un mecanismo de nivel 2 pero también da la opción a las entidades de implementar su propio mecanismo de autenticación nivel 2 el cual será invocado desde la solución.

La Figura 8 presenta el esquema general de autenticación de la solución; se observa que para poder invocar una funcionalidad de riesgo moderado o alto previamente debe haber ingresado a la solución mediante una autenticación de nivel 1 y posteriormente realizar un proceso de autenticación de nivel 2.

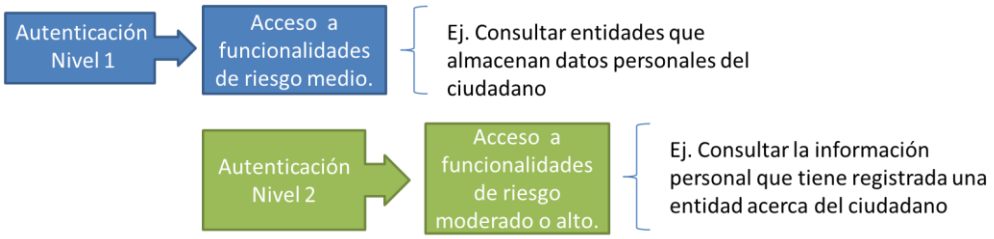

Figura 8. Esquema de autenticación de la solución S1581.

3.2. Descripción de la arquitectura

La arquitectura planteada para la solución S1581 tiene en cuenta los elementos descritos en la sección de autenticación, las funciones presentadas a manera de historias de usuario, consideraciones de uso y de tecnología. Los componentes de la solución se clasifican en 3 paquetes principales orientados a la gestión de datos personales, la autenticación y la administración de la solución.

La Figura 9 sintetiza los componentes de la arquitectura de la solución S1581; la arquitectura propuesta, sugiere la integración de componentes distribuidos tanto en el core de la solución como componente responsabilidad de terceros como la Superintendencia de Industria y Comercio, Gobierno en Línea y las entidades responsables de los datos personales; la Figura 10 esquematiza la distribución de los componentes de acuerdo al responsable de los mismos.

Dentro de los componentes planteados existen algunos a cargo de terceros que actualmente están plasmados como proyectos futuros o en ejecución, este es el caso del Buzón del Ciudadano[102], del Registro Nacional de Base de Datos[3] y del Autenticador en Línea[103]; para efectos del desarrollo de este proyecto se construyeron módulos que simulan el funcionamiento de dichos componentes. En la Figura 10 se pueden identificar los elementos simulados con la etiqueta "(s)". A continuación se describe cada uno de los componentes de la arquitectura propuesta.

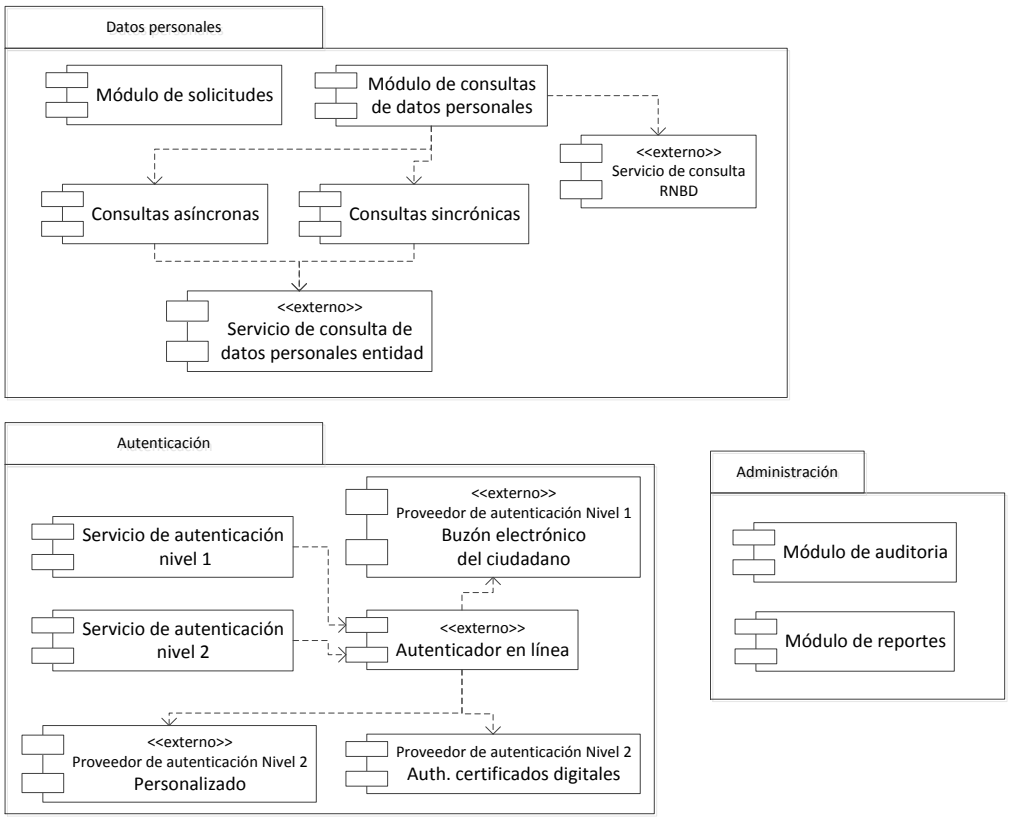

Figura 9. Diagrama de componentes de arquitectura

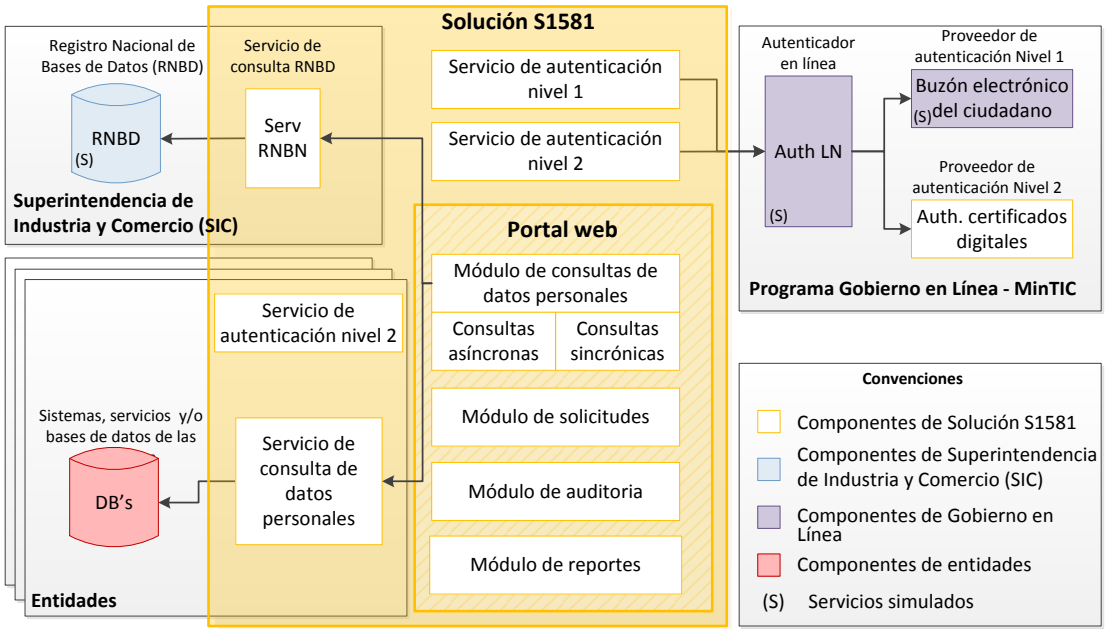

Figura 10. Componentes de la arquitectura de acuerdo a responsables

3.2.1. Componentes de Superintendencia de Industria y Comercio

Los siguientes componentes residen o estarían bajo la supervisión de la Superintendencia de Industria y Comercio (SIC).

A. Registro Nacional de Bases de Datos (RNBD)

Como lo indica la ley 1581, la Superintendencia de Industria y Comercio ha desarrollado el Registro Nacional de Bases de Datos (RNBD), el cual busca ser un directorio público de las bases de datos sujetas a tratamiento que operan en el país[3]. Este componente externo permitirá a la solución S1581 conocer las diferentes bases de datos y las entidades a cargo.

En el RNBD se tendrá acceso, por cada entidad o base de datos, a información como las políticas de tratamiento de datos personales, aviso de privacidad, información del responsable y los datos de contacto para que el ciudadano pueda ejercer sus derechos ante la entidad. En este trabajo se propone extender el registro nacional de bases de datos con el objeto de poder localizar de manera dinámica, servicios informáticos de gestión de datos personales expuestos por las entidades para interactuar con la solución s1581. A continuación se expone cada uno de los atributos extendidos propuestos en este trabajo:

- **URL de servicio de gestión de datos personales (URLSgdp)**: Este atributo describe la dirección para ubicar el servicio. Está compuesto por protocolo, servidor, puerto y ruta del servicio; son definidos como una URL. La Figura 11 presenta mediante un

ejemplo la forma de representar un valor para este atributo. La ausencia de valor para este atributo indica que no existe una implementación del servicio.

Figura 11. Ejemplo de representación de valor para atributo URLSgdp.

- **Versión de Integración:** Permite la descripción de la versión de integración implementada en el servicio (ver definición página 46).En la implementación de este trabajo todos los servicios tendrán la versión 1.0; sin embargo, para futuras mejoras este valor puede cambiar.
- **URL de Autenticación de segundo nivel (URLAuth2N):** Describe la ubicación del servicio de autenticación de segundo nivel que se debe utilizar para la consulta de datos personales. Si la entidad quiere utilizar los servicios de autenticación disponibles en la solución puede indicarlo utilizando los valores "**s1581://auth/n1**" o **s1581://auth/n2** servicio autenticación de nivel 1 y nivel 2 respectivamente.
- **Email de notificación:** Contiene el correo electrónico de contacto de la entidad, a donde serán enviadas las solicitudes tramitadas mediante la herramienta.

Para el desarrollo del proyecto no se tiene acceso directo al Registro Nacional de Bases de Datos, por lo cual se construyó un componente que simula el comportamiento y contenido del sistema. La construcción de este componente ha sido orientada por parte de la Superintendencia de Industria y Comercio.

B. Servicio de consulta RNBD

Esta interfaz hace referencia a un servicio web que se ha desarrollado para interactuar con el Registro Nacional de Bases de Datos; este servicio tendrá como funcionalidades principales consultar el listado completo de bases de datos registradas y la de consultar información específica de una entidad y base de datos. A continuación se listan las operaciones principales de este servicio:

- Consultar las entidades registradas.
- Consultar políticas de protección de datos para una entidad.
- Consultar finalidad del tratamiento de los datos personales.
- Consultar datos de contacto de la entidad: nombre del responsable, correo electrónico de atención, proceso de atención al ciudadano.
- Consultar datos de servicio de gestión de datos personales para solución S1581 (sgdpURL, Versión, auth2NURL, Email de notificación)
- Consultar los sistemas o bases de datos registrados para una entidad.

3.2.2. Componentes de Gobierno en Línea

Los siguientes componentes residen o estaría bajo la supervisión del programa Gobierno en Línea del Ministerio de Tecnologías de la Información y las Comunicaciones.

A. Autenticador en Línea[103][104]

El programa Gobierno en Línea, del Ministerio de Tecnologías de la información y las Comunicaciones, ha desarrollado un conjunto de soluciones para que las entidades puedan prestar servicios en línea[103]; entre estas soluciones se encuentra el autenticador en línea. La plataforma provee herramientas, protocolos y servicios de seguridad que permiten a aplicaciones cliente contactar un conjunto de proveedores de autenticación. Para que sea posible la interacción de estos componentes, es requerido que las partes establezcan una relación de confianza en donde el proveedor esté dispuesto a prestar el servicio y los clientes confíen en el mecanismo utilizado.

La Figura 12 presenta el esquema general de interacción de los componentes del sistema Autenticador en línea; en él se observa que la aplicación A tiene una relación de confianza con Z y utiliza sus servicios de autenticación.

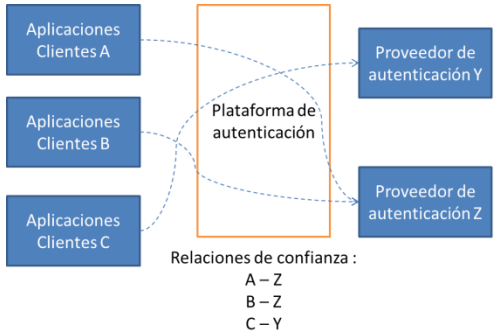

Figura 12. Esquema de interoperabilidad del sistema Autenticador en línea[104].

Los proveedores pueden incluir mecanismos de autenticación como usuario y contraseña, certificados digitales de entidades abiertas, certificados digitales de entidades cerradas, datos biométricos, entre otros. La solución S1581 actúa como un cliente de la plataforma Autenticador. No se tiene acceso directo al componente, por lo cual en el proyecto se creó una aplicación que simula este sistema.

B. Buzón electrónico del ciudadano[105][102]

Dentro de los futuros proyectos planteados por Gobierno en línea para apoyar las tecnologías de información en el país, se encuentra el poder contar con un sistema de buzón electrónico del colombiano. Este buzón actuará como un correo electrónico en el cual una persona pueda recibir toda su información relacionada con entidades del estado[102]. Actualmente existe la plataforma "tramitador en línea" la cual presenta un servicio de notificación en la cual también se puede relacionar una cuenta de correo con un ciudadano o entidad[105], el buzón del ciudadano complementaria dicha iniciativa.

El buzón electrónico será personal e intransferible y asignado exclusivamente al titular; aun no existen detalles de cómo será el proceso de asignación. Sin embargo, desde este proyecto se plantea que la entrega debe tener en cuenta un proceso inicial en donde el ciudadano se acerque a un punto de atención, a cargo de una entidad de validación, y pueda solicitar su buzón; La entidad de validación se consideraría como un tercero confiable que tendría la tarea verificar la identidad de la persona antes de asignar el buzón al ciudadano.

El buzón electrónico emplea un usuario y contraseña para realizar el proceso de autenticación, de esta manera se presenta una oportunidad para que la solución S1581 lo utilice como un proveedor de autenticación de fácil acceso al ciudadano. El buzón es utilizado en el servicio de autenticación de primer nivel de la solución S1581 y es accedido mediante la plataforma Autenticador en línea. Este componente será simulado ya que aún no existe una implementación del buzón electrónico del ciudadano.

3.2.3. Componentes de Entidades Responsables de Datos Personales

Los siguientes componentes residen o estaría bajo la supervisión de las entidades responsables de datos personales.

A. Servicio de autenticación nivel 2 implementado por entidad

En caso en el que la entidad considere que el mecanismo de autenticación de nivel 2 provisto por la solución S1581 no es suficiente para sus requerimientos de seguridad, puede implementar su propio servicio bajo los parámetros descritos en la sección de definición de integraciones (Ver página 50). La solución podrá invocar los servicios de autenticación personalizados siempre y cuando hayan sido construidos bajo los lineamientos establecidos en el presente trabajo y que la entidad registre la información de ubicación del servicio en el Registro Nacional de Bases de Datos.

B. Sistemas, servicios y/o bases de datos de las entidades

Son aquellos elementos informáticos donde residen o pueden ser tratados los datos personales de los ciudadanos, estos elementos son el objeto de revisión y control descrito en la Ley 1581 de 2012. Para la implementación de la solución S1581 se considera que es el insumo a partir del cual las entidades pueden entregar la información que les sea solicitada para cumplir con la misma Ley.

La solución S1581 no tendrá acceso directo a los sistemas o repositorios de información, por el contrario se plantea que se construyan servicios de información que permitan la interacción con estos ítems.

Para el desarrollo del proyecto se ha desarrollado una integración con una entidad real que permitió realizar la validación de la solución (ver sección 6.1 del capítulo IV -).

3.2.4. Componentes centrales de solución informática S1581

Los siguientes componentes conforman los servicios centrales de la solución informática S1581, son los encargados de responder a los ciudadanos e interactuar con los componentes a

cargo de terceros como la Superintendencia de Industria y Comercio, el Programa Gobierno en Línea y las entidades responsable de los datos personales.

A. Servicio de autenticación nivel 1

La solución S1581 tiene un servicio de autenticación nivel 1 que se utiliza para el ingreso a la solución y las funcionalidades expuestas en el diseño de la autenticación. Este servicio utilizará el servicio "Autenticador en línea" desarrollado por el programa Gobierno en Línea[103] para utilizar el proveedor de autenticación "buzón electrónico del ciudadano". La identidad del ciudadano se establecerá mediante la validación de las credenciales en su buzón electrónico.

B. Servicio y proveedor de autenticación Nivel 2.

El mecanismo de autenticación de nivel 2 estará sujeto a los requerimientos de seguridad que la entidad encargada de los datos personales establezca; sin embargo la solución S1581 provee un servicio de autenticación basado en certificados digitales que está disponible para aquellos casos en los que se considere que es apropiado utilizar este método.

Este servicio mediante el uso de la plataforma "Autenticador en Línea" accederá a un proveedor de autenticación quien realmente realizará la tarea de verificación y validación de la identidad mediante el certificado digital.

Tanto el servicio como el proveedor de autenticación nivel 2, han sido desarrollados para cumplir con los requerimientos de este proyecto.

C. Servicio de consulta de datos personales de las entidades

Se plantea que cada entidad que quiera hacer parte de la solución S1581, debe implementar un servicio de consulta de datos personales. Este servicio será el encargado de interactuar con los sistemas, servicios y bases de datos internas de la entidad y extraer la información solicitada por el ciudadano; es requerido que se cumpla con los lineamientos planteados en la sección de descripción de integraciones (Ver página 48). Las siguientes son las operaciones a implementar en este servicio:

- Verificar tratamiento de datos: permite identificar si la entidad realiza tratamiento de datos de un individuo.
- Consulta de datos de personales de un individuo: se extrae los datos personales que la entidad gestiona de un individuo. Se excluyen los datos sensibles. Dentro de este componente las entidades pueden adicionalmente incluir elementos como los fines del tratamiento de datos y la autorización otorgada por el ciudadano.

D. Módulo de consultas de datos personales

Mediante este componente la solución S1581 puede gestionar todas las consultas de los ciudadanos, incluyendo las entidades que tiene su información personal y el acceso al detalle de sus datos personales. Algunas de las consultas no son apropiadas para ejecutarlas en modo online dado que pueden tardar un tiempo considerable; es el caso de la búsqueda de entidades

que tiene información personal de un ciudadano; por esta razón se apoya en 2 submódulos los cuales se explican a continuación:

- **Submódulo de consultas asíncronas:** Permite la gestión de consultas que toman un tiempo largo para ser procesadas. El flujo inicia cuando el módulo de consultas de datos personales crea una tarea de consulta asíncrona, inmediatamente el control de la aplicación será devuelto aun cuando la tarea no ha sido terminada. El procesamiento de la tarea se realiza tras bambalinas mientras el usuario puede seguir interactuando con la aplicación o incluso saliendo de la misma. Una vez terminado el proceso se informará al usuario, mediante un correo electrónico, para que pueda consultar el resultado.
- **Submódulo de consultas sincrónicas:** Componente enfocado a ejecutar consultas que requiere una respuesta inmediata. El flujo inicia cuando el módulo de consultas de datos personales crea una tarea de consulta sincrónica, esta será procesada inmediatamente por la solución y presentada al usuario en línea.

E. Módulo de solicitudes

La solución S1581 contempla que los ciudadanos envíen solicitudes mediante correo electrónico de rectificación de información y revocación de autorización. Este componte permitirá la gestión de recepción de la solicitud y su envío mediante correo electrónico a la entidad específica.

F. Módulo de auditoria

Este módulo es transversal al resto de componentes de la solución; permite llevar una bitácora de todas las acciones realizadas por un ciudadano dentro de la solución. El registro de eventos se realizará sobre el repositorio de la solución lo cual permitirá posteriormente realizar consultas sobre la bitácora.

G. Módulo de reportes

Este elemento permitirá tanto al ciudadano como a la Superintendencia de Industria y Comercio y a las entidades consultar información sobre el uso de la solución, de las consultas y solicitudes realizadas. A continuación se presenta los reportes contemplados:

- Búsquedas realizadas por un ciudadano en un periodo de tiempo. Usuario: ciudadano, Superintendencia de Industria y Comercio (SIC).
- Consultas realizadas a una entidad en un periodo de tiempo. Usuario: Entidad, Superintendencia de Industria y Comercio (SIC).
- Solicitudes realizadas por un usuario en un periodo de tiempo. Usuario: ciudadano, Superintendencia de Industria y Comercio (SIC).
- Solicitudes realizadas a una entidad en un periodo de tiempo. Usuario: Entidad, Superintendencia de Industria y Comercio (SIC).
- Consultas realizadas a entidades en un periodo de tiempo. Usuario: Superintendencia de Industria y Comercio (SIC).

- Solicitudes realizadas a entidades en un periodo de tiempo. Usuario: Superintendencia de Industria y Comercio (SIC).

3.3. Diagrama de entidades de negocio

La solución S1581 contempla el uso de entidades de negocio (*EntityBean*, ver página 24) como la base de lógica de negocio, en esta solución no todas las entidades serán persistentes en la base de datos local ya que algunas serán solicitadas mediante servicios de integración a componentes externos (ver página 37, Descripción de la arquitectura). La Figura 13 muestra el diagrama de las entidades principales de la solución y enmarca en anaranjado aquellas que son persistentes en la base de datos local.

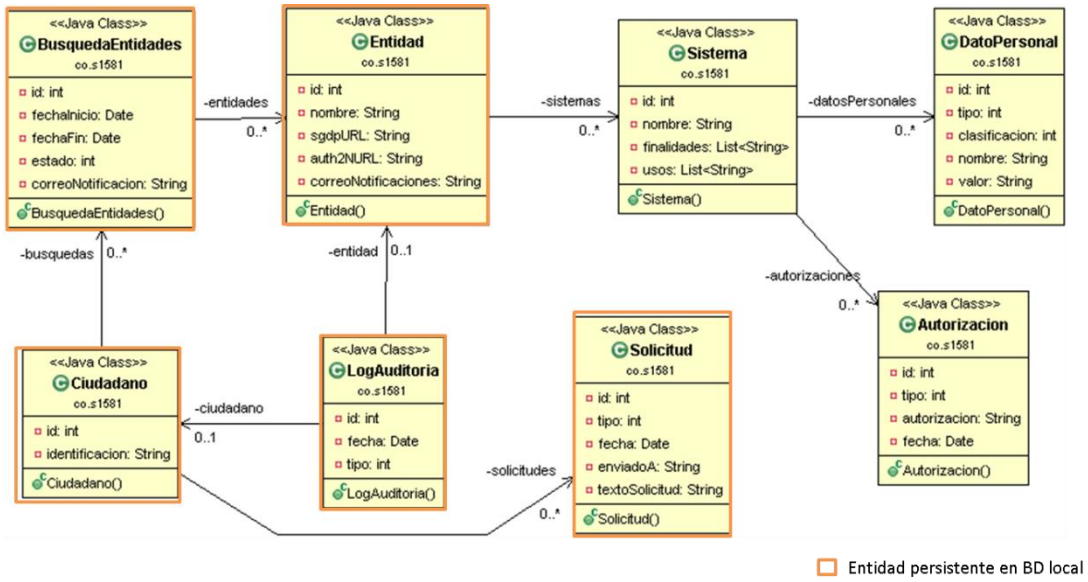

Figura 13. Diagrama de clases de entidades de negocio para solución S1581

3.4. Descripción de entidades de negocio

Ciudadano: Esta entidad representa a un ciudadano, se utiliza la mínima información para establecer la identidad de la persona y poder interactuar con los mecanismos de autenticación y consulta de la solución S1581. De acuerdo las funcionalidades planteadas en las Historias de Usuario, esta entidad tendrá relación a búsquedas, solicitudes y registros de auditoria del sistema. Esta entidad de negocio es persistente.

BusquedaEntidades: Representa la consulta del ciudadano para obtener las entidades que tienen sus datos personales. Esta búsqueda se realizara de manera asincrónica por lo que es requerido poder contar con información como la fecha de inicio y fin del proceso, y el estado del mismo. Como resultado se obtendrá un conjunto de entidades. Esta entidad de negocio es persistente.

Entidad: Representa organizaciones o instituciones que están registradas en el Registro Nacional de Bases de Datos (RNBD) y que han sido retornadas como el resultado de una búsqueda del ciudadano. Esta entidad de negocio es persistente.

Sistema: Caracteriza los repositorios, bases de datos, sistemas de información, plataforma de software, etc. Que permita el tratamiento de datos personales de acuerdo a lo dispuesto en la Ley 1581 de 2012. La información de esta entidad de negocio se obtiene mediante el "Servicio de consulta RNBD" expuesto en la sección anterior, inicialmente NO es persistente, sin embargo fue necesario implementar un mecanismo de cache para optimización de la solución S1581.

DatoPersonal: Esta entidad de negocio contempla cada uno de los datos personales del ciudadano gestionados por un sistema. Un DatoPersonal se describirá mediante su nombre y clasificación como biográfico, sensible, laboral, salud, académico, etc. El dato personal tendrá un valor el cual es representado en XML para dar flexibilidad al uso de datos compuestos. Esta entidad de negocio NO es persistente.

Autorización: Describe la autorización dada por el ciudadano a una entidad para poder tratar sus datos personales; incluye el texto que comprende la autorización, la fecha en la cual se otorgó e información de cómo fue capturada. Esta entidad de negocio NO es persistente.

Solicitud: La solución S1581 contempla funcionalidades que permiten el envío de solicitudes por parte del ciudadano a diferentes entidades o a la misma Superintendencia de Industria y comercio (SIC). Esta entidad de negocio mantendrá el registro de cuando se realizó la solicitud, a quien fue enviada y el texto que contemplo dicha solicitud. Esta entidad de negocio NO es persistente.

LogAuditoria: mediante esta entidad de negocio se registran todos los eventos e interacciones del ciudadano en la solución. Se contempla registros que representan la creación de una búsqueda de entidades, la consulta a una entidad pos los datos personales, el envío de una solicitud, entre otros. Esta entidad de negocio es persistente.

3.5. Tecnologías seleccionadas

La solución S1581 se implementó bajo el leguaje de desarrollo Java. Se decidido utilizar JBoss Developer Framewok dado que permite hacer uso de las tecnologías actuales en el mercado, además como proyecto cuenta con soporte y documentación que serán mantenidos a largo plazo (ver sección 4.3 del marco teórico) . La siguiente tabla resume las tecnologías y frameworks utilizados.

Ítem	**Tecnología / Versión**
Lenguaje de programación	Java SDK 1.7 / JEE6
Framework de desarrollo web	- JBoss Developer Framework (jdf 2.1): Asynchronous JavaScript and XML (AJAX), JavaServer Faces (JSF 2) / RichFaces 4.1, Java Persistence (JPA 2) , Enterprise Java Beans (EJB 3.1) - PrimeFaces 4.0
Motor de Base de datos	MySQL Community Server 5.6

	Nota: Es posible utilizar otros motores de BD, ya que se utiliza framework de persistencia JPA. Sin embargo, no han sido probados.
Servidor de aplicaciones	JBoss Application Server 7.1 (JBoss AS 7.1)
Servicios Web	JavaTM API for XML-Based Web Services (JAX-WS) 2.0 WSS(WS-Security)
Autenticación	OpenID 2.0
IDE de desarrollo	Eclipse Java EE IDE for Web Developers, Version: Kepler

Tabla 7. Tecnologías utilizadas en S1581

4. Especificación de interfaces de integración

La solución informática S1581 presenta dos tipos de integraciones, por una parte se incluye el consumo de información de diferentes fuentes de datos y de otra el uso de diferentes mecanismos de autenticación. A continuación se describe cada uno de los elementos de integración.

4.1. Integración con diferentes fuentes de datos

La solución informática está constituida por varias integraciones para consulta y consumo de datos, como se describió en el capítulo 3.2 Descripción de la arquitectura; estas integraciones se realizan mediante Servicios Web. Se consideró utilizar *Java API for XML Web Services (JAX-WS)*[10][5] y *RESTful Web services (JAX-RS)*[5] como tecnologías para la implementación de servicios web.

Dado que para la implementación de este proyecto un factor fundamental es la seguridad se decidió utilizar servicios basados en SOAP con la implementación *JAX-WS*[10][5] (Ver descripción y características de SOAP y RESTful en marco teórico). En las siguientes secciones se describe la forma en la cual se debe implementar un servicio Web para la solución S1581.

4.1.1. Parámetros de entrada y salida de Servicios Web

Los parámetros utilizados en los Servicios Web de la solución S1581 deben ser definidos como tipos de datos primitivos soportados en JAX-WS, la siguiente tabla resume algunos de los tipos de datos más representativos, indicando su tipo en forma de esquema XML y su representación en Java[10]:

Tipos de esquema XML	Tipo de Dato Java
`xsd:string`	`java.lang.String`
`xsd:int`	`Int`
`xsd:long`	`Long`
`xsd:float`	`Float`

[10] La lista completa de datos soportados JAX-WS se puede consultar en The Java EE 6 Tutorial[5] en la tablas 19-1 y 19-2.

xsd:boolean	boolean
xs:dateTime	java.util.Date

Tabla 8. Tipos de datos primitivos JAX-WS, adaptado de [5].

Para los casos en los que se requiere manejo de estructuras de datos, se definió utilizar la representación *JavaScript Object Notation* - Notación de Objetos de JavaScript (JSON)[7].

En las siguientes secciones se utiliza la notación *JSON Schema*[91] para describir la estructura del mensaje JSON.

4.1.2. Especificación Servicio de consulta RNBD

Las operaciones del servicio de consulta del Registro Nacional de Bases de Datos (Ver sección 3.2.1 Componentes de Superintendencia de Industria y Comercio) se unificaron en un único método de consulta de entidades registradas. Este método tiene los siguientes elementos:

- **Nombre**: consultarEntidades.
- **Solicitud**: sin parámetros.
- **Respuesta**: String en formato json que representa un arreglo de entidades.

La Tabla 9 presenta la especificación del mensaje en notación JSON Schema, en ella se observa que la respuesta es un arreglo de objetos llamado entidades, en el cual cada elemento trae información como nombre, id, URLServicio, URLAuth2N, mailNotificacion etc. La Tabla 10 presenta un ejemplo del mensaje de consulta de entidades en el cual se obtiene una sola entidad con el nombre "Pontificia Universidad Javeriana".

```
{ "type":"object",
  "description": "Representación de consulta de entidad",
  "id": "http://s1581.com", "required":false,
  "properties":{
    "entidades": {
      "type":"array", "id": "http://s1581.com/entidades",
      "required":true,
      "items":
      { "type":"object",
        "name": "entidad",
        "required":false,
        "properties":{
          "nombre": { "type": "string", "required": true },
          "id": { "type": "string", "required": true },
          "URLServicio": { "type": "string", "format": "uri" },
          "URLAuth2N": { "type": "string", "format": "uri" },
          "mailNotificacion" : { "type": "string", "required": false },
          "direccion" : { "type": "string", "required": false },
          "telefono" : { "type": "string", "required": false },
          "responsable" : { "type": "string", "required": false },
          "imaURL": { "type": "string", "format": "uri" },
          "UrlAvisoPrivacidad": { "type": "string", "format": "uri" },
          "versionIntegracion": { "type": "string", "required": true }
} } } } }
```

Tabla 9. Esquema JSON para respuesta consultar las entidades registradas

```
{ "entidades":
  [{"nombre":"Pontificia Universidad Javeriana",
    "id":"11111",
    "URLServicio":"https://www.javeriana.edu.co/sgdp",
    "URLAut2N":"https://www.sinesat.com/auth2N",
    "mailNotificacion":"contacto@javeriana.edu.co",
    "direccion":"KR 7 # 40-62, Carrera 7, Bogotá",
    "telefono":"3208320",
    "responsable":"Padre Joaquín Sánchez García SJ.",
    "imaURL":"http://www.javeriana.edu.co/logo.png",
    "UrlAvisoPrivacidad":"http://www.javeriana.edu.co/AvisoPrivacidad",
    "versionIntegracion":"1.0"} ] }
```

Tabla 10. Ejemplo JSON para respuesta de consultar las entidades registradas

4.1.3. Especificación Servicio de consulta de datos personales de las entidades

A continuación se describe las operaciones del servicio de consulta de datos personales de las entidades. Para cada una de ellas se indicara nombre de la operación, parámetros de solicitud y respuesta, y el esquema JSON utilizado para interpretar los datos trasmitidos.

A. Verificar tratamiento de datos

- **Nombre operación**: isResponsableDatosPersona.
- **Solicitud**: docId: String. Documento de identidad de la persona.
- **Respuesta**: Booleano, un valor verdadero indica que la entidad si trata datos de la persona y es responsable de ellos; un valor falso indica que no existe tratamiento de los datos para esta persona por parte de la entidad.

B. Consulta de datos de personales de un ciudadano

- **Nombre operación**: getDatosPersonales.
- **Solicitud**: docId: String. Documento de identidad del ciudadano.
- **Respuesta**: String en formato json que representa un arreglo de Datos personales.

La Tabla 11 presenta la especificación del mensaje en notación JSON Schema, en ella se observa que la respuesta es un arreglo de objetos llamado datospersonales, en el cual cada elemento que representa un dato personal trae la siguiente información:

- **Nombre**: Referencia el dato personal, como por ejemplo apellido, cedula, fecha de nacimiento, etc.
- **Clasificación**: indica la clasificación del dato personal. Esta clasificación puede tener varios niveles (Ver página 28 taxonomía de datos personales), el primer nivel debe ser por defecto "datos_personales ", los siguientes niveles dependerán de la clasificación de la entidad. La jerarquía se representarse como una cadena la cual concatena los diferentes niveles utilizando el signo punto como separador. Por ejemplo para representar un dato de tipo biográfico la clasificación será: datos_personales.biográficos.

- **Tipo**: En esta versión se soporta 2 tipos de datos: String (S) o Archivo (F); la mayoría de datos personales podrán ser representados como string, a futuro se pueden ampliar a otros tipos de datos. El tipo de datos archivo puede representar elementos como fotos, hojas de cálculo, pdf's, etc.
- **Valor**: valor asociado al dato personal,
- **Sensible**: atributo booleano (true o false) que indica si el dato personal es de carácter sensible.
- **Mime**: para datos de tipo archivo, es posible indicar el tipo de archivo asignando el mime. Por ejemplo para enviar una imagen se puede utilizar la mime "image/jpeg".
- **FileName**: indica el nombre del archivo
- **File**: datos del archivo en formato binario.

```
{ "type":"object",
  "description": "Representación de consulta de datos personales",
  "id": "http://s1581.com", "required":false,
  "properties":
  { "datospersonales":
    { "type":"array", "id": "http://s1581.com/categorias",
      "required":true,
      "items":
      { "type":"object", "name": "datopersonal", "required":false,
        "properties":
        { "nombre": { "type": "string", "required": true },
          "clasificacion": { "type": "string", "required": true },
          "tipo": { "type": "string", "required": true },
          "valor": { "type": "string", "required": true },
          "sensible": { "type": "boolean", "required": true },
          "mime": { "type": "string", "required": false },
          "fileName": { "type": "string", "required": false },
          "fileNfileame": { "type": "byte[]", "required": false }
        } } } } }
```

Tabla 11. Esquema JSON para respuesta consulta de datos personales de un ciudadano.

La Tabla 12 presenta un ejemplo de la respuesta del mensaje de consulta del detalle de datos personales de un ciudadano. En este ejemplo, "CARLOS ANDRES CAMARGO BEDOYA" tiene tres datos personales: nombre, fecha de nacimiento y foto; tanto el nombre como la fecha de nacimiento son de tipo String y están clasificados en la categoría "datos_personales.biográficos". Por su parte el dato personal foto es de tipo archivo (F), el atributo "mime" tiene valor "image/jpeg" indicando que este archivo hace referencia a una imagen.

```
[ {  "nombre":"Nombre",
  "clasificacion":"datos_personales.biograficos",
  "tipo":"S",
  "valor":"CARLOS ANDRES CAMARGO BEDOYA",
  "sensible":false
  },{"nombre":"Fecha de nacimiento",
  "clasificacion":"datos_personales.biograficos",
  "tipo":"S",
  "valor":"1982-10-13",
  "sensible":false
```

```
},{"nombre":"Foto",
"clasificacion":"datos_personales.geneticos.fotos",
"tipo":"F",
"sensible":false,
"mime":"image/jpeg",
"fileName":"foto3.png",
"file":[-119,80,...,78,39] } ]
```

Tabla 12. Ejemplo JSON para respuesta de consulta de datos personales.

4.1.4. Seguridad de Servicios Web

Todos los servicios web de la solución S1581 deben cumplir con los siguientes parámetros de seguridad:

- La comunicación entre servicios de información y la solución informática S1581 debe realizarse bajo protocolo seguro https.
- Cada proveedor de servicios de identidad debe autenticar el acceso utilizando certificados digitales, estos proveedores deben registrar el certificado digital de la solución informática S1581.
- Cada proveedor de servicios de identidad debe proveer un certificado valido y reconocido por una entidad de certificación confiable. La solución informática S1581 incluye un almacén de certificados de servicios, el cual es consultado para permite realizar la autenticación de estos componentes.

Si además del cifrado del canal y autenticación extremo a extremo, se requieren otros elementos de seguridad como firma de mensaje y cifrado de campos en mensaje SOAP, puede incluirse propiedades bajo el estándar WS-Security (WSS)[67].

4.2. Proveedores de Autenticación

La solución S1581 provee un mecanismo de autenticación de primer nivel y uno de segundo nivel; sin embargo, cada entidad puede proveer su propio mecanismo de autenticación de acuerdo a sus necesidades particulares. Para lograr esta interacción se utiliza el estándar OpenID[9].

De acuerdo al estándar OpenID existe una parte que confía (*Relying party RP*) quien ejerce el papel de cliente de un servicios de autenticación y otra parte proveedora de identidad (*OpenId providers OP*)[9]. En este caso la solución S1581 actúa como RP y cada servicio de autenticación será visto como un OP. En el marco teórico se encuentra una descripción de OpenID. El proceso de autenticación de la solución se divide en nueve pasos, en los cuales se solicita al usuario la información de validación y es finalmente el proveedor de autenticación quien realiza la tarea de verificación de la identidad. La Figura 14 resume los pasos del proceso de autenticación.

Para la construcción de un servicio de autenticación compatible con la Solución S1581 se debe seguir la especificación OpenID Authentication 2.0[106], si este servicio se está cons-

truyendo con lenguaje java puede utilizarse la librería OpenID4Java (OpenID for java)[107] la cual implementa las principales características y requerimientos del protocolo.

OpenID contempla que en la respuesta del *OpenID provider* hacia el *Relying party* se puede devolver información del usuario autenticado utilizando la especificación *"OpenID Attribute Exchange* 1.0"[108]; los proveedores de autenticación compatibles con la solución informática S1581 deben regresar en su respuesta los campos:

- Documento de identidad: este campo es obligatorio en la respuesta.
- Correo electrónico: este campo es obligatorio para servicio autenticación de nivel 1 y opcional para servicio autenticación de nivel 2.

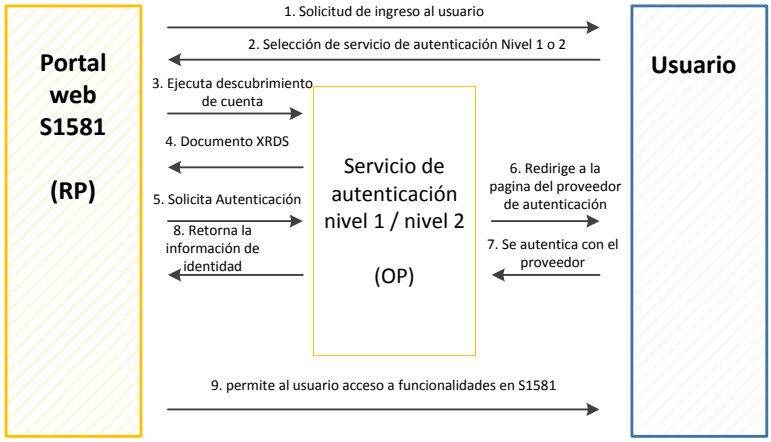

Figura 14. Pasos de autenticación de S1581 utilizando OpenID, adaptado de [109].

5. Descripción de la solución informática s1581

En el presente trabajo se construyó la solución informática s1581 en la cual desarrollaron seis proyectos que se describen en la Tabla 13, utilizando el entorno de desarrollo integrado (IDE) Eclipse versión *Kepler Service Release 1*[110]. Para lograr los objetivos de seguridad enfocados a autenticación del ciudadano y autenticación mutua entre servicios de información con certificados digitales fue necesario realizar configuraciones sobre los contenedores de aplicación, para lo cual se utilizó JBoss Application Server 7.1 (JBoss AS 7.1). La Figura 15 presenta el diagrama de despliegue de los diferentes componentes de la solución.

Proyecto	Descripción
s1581AuthN1	Este proyecto contiene los componentes desarrollados para la autenticación de nivel 1. Simula los componentes de buzón del ciudadano y autenticador en línea. El mecanismo empleado para autenticación es usuario y contraseña.
s1581AuthN2	Contiene los componentes desarrollados para la autenticación de nivel 2. El mecanismo utilizado es el de autenticación con certificados digitales.
s1581	Es el proyecto principal el cual contiene los componentes centrales de la solución informática y representa el portal del ciudadano.
RNBD	Mediante este proyecto se simula el Registro Nacional de Bases de Datos

Entidades	Mediante este proyecto se representa la integración con entidades para acceso a los servicios de información.
Javeriana	Como parte de la validación se implementó la integración con la Pontificia Universidad Javeriana para consulta de datos personales, este proyecto contiene desarrollo realizado (ver página 57).

Tabla 13. Descripción de proyectos de la solución en IDE Eclipse

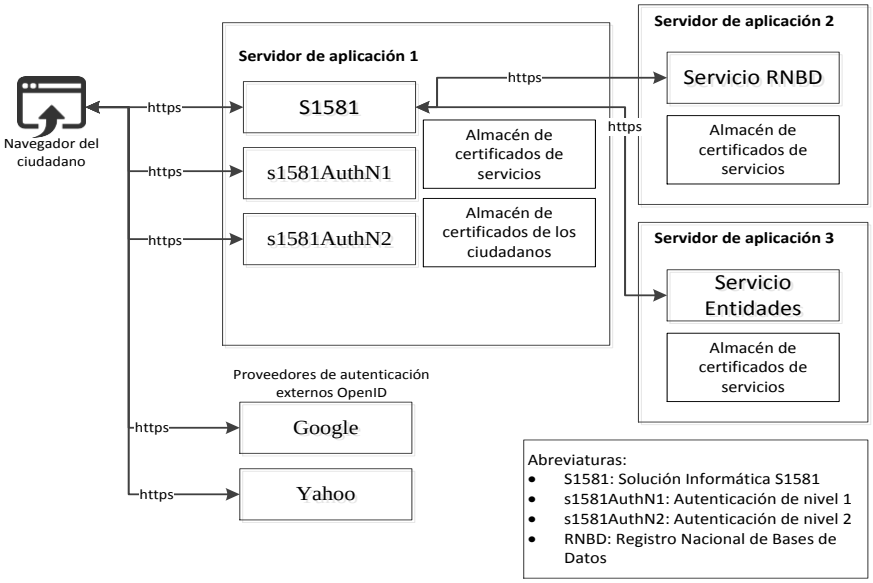

Figura 15. Diagrama de despliegue de la solución informática S1581

A continuación se describen los detalles más relevantes del desarrollo.

5.1. Autenticación de nivel 1 y 2

En el proyecto *s1581AuthN1* se desarrollaron las funcionalidades que permiten la autenticación nivel 1 basada en usuario y contraseña. Este sistema tiene una relación de correo electrónico y documento de identidad para simular el buzón del ciudadano y efectuar las tareas de autorización, la autenticación se delega al proveedor de correo electrónico en este caso Gmail y Yahoo!. Se empleó el mecanismo OpenID[66] en 2 vías; por una parte para ser invocado por la solución informática S1581, actuando como proveedor de autenticación y de otra parte operando como cliente para invocar un proveedor OpenID externo. La Figura 16 muestra las pantallas de autenticación del proveedor externo.

El componente de autenticación solicita al proveedor externo el correo electrónico para cotejarlo con el repositorio de los ciudadanos; algunos de los proveedores solicitarán la autorización al usuario para realizar esta tarea, como se muestra en la Figura 16 para el caso de google.

Por otro lado, el proyecto *s1581AuthN2* contiene las funcionalidades que permiten la autenticación de nivel 2 basada en certificados digitales. El sistema tiene un registro del ciudadano que relaciona el documento de identidad con el nombre distintivo del certificado, por ejemplo para el ciudadano Carlos Camargo se tendría la relación: {11366031, *CN=carlos-camargo, OU=bog, O=ciudadano, ST=gov, C=CO* } La autenticación nivel 2 utiliza OpenID para ser invocado por la solución informática S1581como proveedor de autenticación, este componente también puede ser utilizado para realizar autenticación de nivel 1.

Figura 16. Pantallas de proveedor de autenticación externo nivel 1

El proceso de validación de certificados digitales se realiza mediante un dominio de seguridad del contenedor de aplicaciones que ha sido configurado para consultar el almacén de llaves de confianza (*truststore*) donde están los certificados de los ciudadanos; en el anexo 4 se describe el proceso de configuración de este componente. Para acceder a las funcionalidades de riesgo moderado o alto los ciudadanos deben tener instalada la llave privada de su certificado digital en el navegador en el que están realizando el proceso. La Figura 17 muestra la pantalla presentada en Internet Explorer para la autenticación de nivel 2 con certificados digitales.

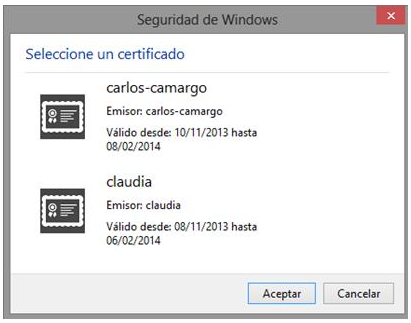

Figura 17. Pantalla de autenticación nivel 2 con certificados digitales

5.2. Solución informática S1581

El *core* de la solución informática S1581, ha sido desarrollado en un esquema de 3 capas utilizando las bondades de *Java Platform, Enterprise Edition 6* (JEE6)[5]. En la capa de persistencia se crearon entidades de negocio con JPA (*Java Persistence API*), en la capa de lógica de negocio se utilizó EJB´s (Enterprise JavaBeans) para un control mediante componentes; Asimismo se explotaron algunas de las novedades que trae la versión 6 de JEE, como son la invocación asíncrona de métodos y los timer-services; en esta capa también se incluyeron los clientes de servicios web para invocar servicios al Registro Nacional de Bases de Datos y a las Entidades. Para finalizar en la capa de presentación se implementó JavaServer Faces (JSF) mediante los framewoks RichFaces y PrimeFaces,

La interfaz de usuario se diseñó teniendo en cuenta criterios de usabilidad y accesibilidad para el ciudadano (Ver manual del usuario). Desde el menú principal se obtiene acceso a funcionalidades, tales como: buscar entidades, consultar entidades, revisar solicitudes de rectificación y revocación, revisar bitácora de auditoria, entre otras; también se encuentra la identificación del usuario y acceso a links referentes a Protección de Datos Personales(Ver manual del usuario).

Desde esta interfaz los pasos a seguir por un usuario para acceder a sus datos personales son los siguientes:

a. Seleccionar “buscar entidades”, allí el ciudadano podrá iniciar una solicitud asíncrona para la búsqueda de entidades que tienen sus datos personales podrá seguir navegado en la aplicación o incluso salir. Al finalizar el proceso de búsqueda el ciudadano recibirá un correo de notificación indicando este hecho. Sobre esta opción se invoca el servicio de información de las entidades que permite identificar si tienen o no información de un ciudadano específico.
b. Seleccionar “consultar entidades”, en esta opción aparece la lista de entidades identificadas en la búsqueda. Al seleccionar alguna de ellas se muestran los datos de contacto y el aviso de privacidad de la entidad.
c. Sobre una entidad el usuario puede escoger la opción “Ver mis datos personales”, en este momento se invoca el servicio de información de la entidad que permite obtener el listado de dicha información. Se presenta en la pantalla 3 opciones “Consulta Estándar”, “Navegación por Taxonomía” y “Estadísticas”. Desde esta interfaz el ciudadano podrá conocer sus datos personales utilizando herramientas de filtrado y navegación.

De acuerdo a la clasificación de datos realizada por la entidad, orientada por la taxonomía planteada en este proyecto, S1581 presenta dinámicamente la información; En la vista estándar los datos personales son organizados en filas como se muestra en la imagen izquierda de la Figura 18. Desde esta funcionalidad el usuario puede filtrar los datos por categorías, en la imagen de la derecha de la Figura 18 se presenta un ejemplo en el cual se han filtrado datos de tipo “genético” en donde se clasifican las fotografías.

Como se describió en la sección de integraciones la solución informática puede presentar información de tipo “cadena de caracteres” o “archivo”; para el caso de archivos, S1581 iden-

tifica si se trata de una imagen y es capaz de presentarla gráficamente, en caso contrario se muestra un link para descarga.

Se contempló una segunda forma de consulta de datos personales denominada "Navegación taxonomica", esta funcionalidad fue desarrollada con el objeto de poder consultar la información de acuerdo a la jerarquia de clasificación dada por la entidad. Esta funcionalidad permite identificar facilmente propiedades de los datos personales, por ejemplo identificar datos sensibles, reconocer la relación de un dato con otros de su misma clasificación, y representar datos estructurados.

Figura 18. Consulta de detalle de datos personales

Para lograr la "navegación taxonomica" los datos personales son representados como un arbol n-ario como se observa en la Figura 19; el nodo raiz es la clasificación genérica "dato_personal" representado con color naranja; cada categoria es presentada como un nodo de color azul, el cual puede contener datos personales u otras categoias. Finalmente los datos personales son representados como nodos hoja, son de color rojo si se refiere a datos sensibles o de color verde en otro caso.

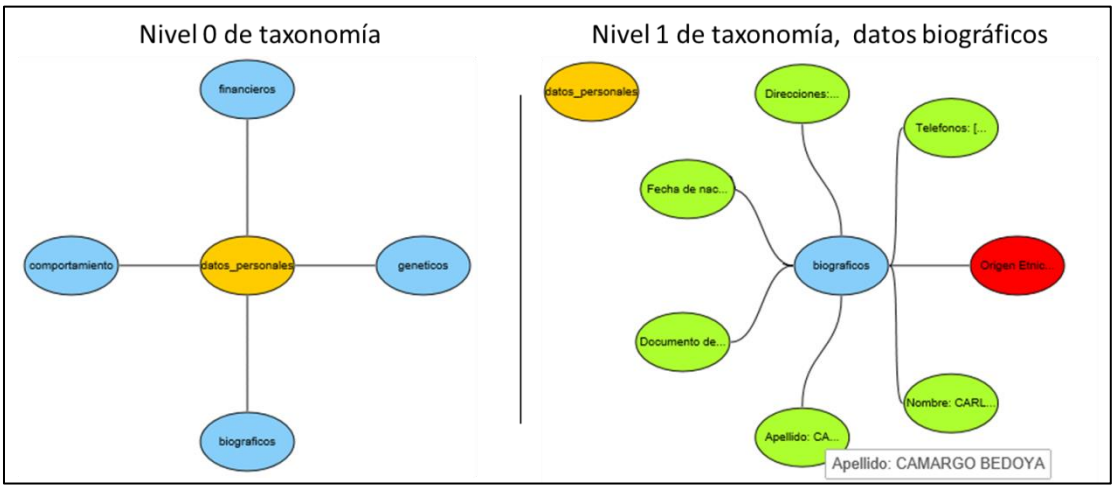

Figura 19. Navegación taxonomica de datos personales

En el ejemplo de la Figura 19, en el nivel cero se observan cuatro categorias: datos personales de tipo biográficos, genéticos, financieros y de comportamiento; en el nivel 1 se observan los datos personales de tipo biográfico donde se identifica que hay un dato sensible que es "Origen Etnico" y que el apellido del ciudadano es "CAMARGO BEDOYA".

Finalmente, el componente de consulta de detalle de datos personales cuenta con una opción de consulta de estadísticas que permite identificar el número de datos personales por categoría indicando cuales de estos son sensibles. El objetivo de estas estadísticas es que el ciudadano pueda valorar la información que tiene la entidad acerca de él, en particular en lo relacionado con datos sensibles.

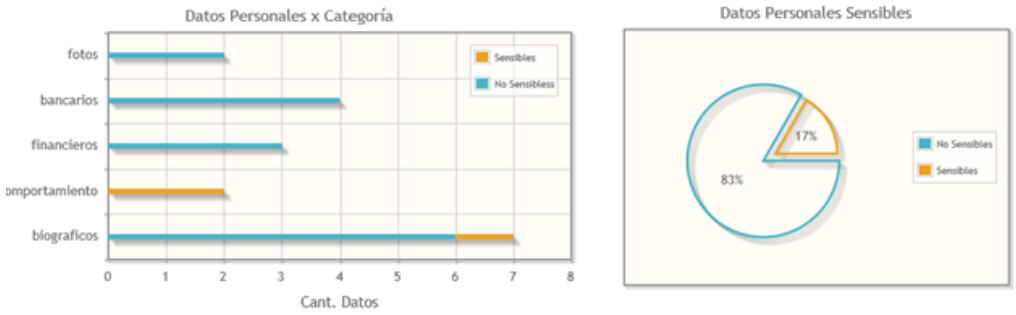

Figura 20. Estadísticas de datos personales

La solución informática S1581 cuenta con otras funcionalidades como la de radicar solicitudes de rectificación o revocación, revisar el listado de búsquedas de entidades, y consultar la bitácora de eventos para revisar la actividad del ciudadano. Para ampliar la información sobre las funcionalidades de la solución consultar el manual del usuario.

6. Validación de la Solución Informática S1581

S1581: Solución informática de gestión de datos personales del ciudadano colombiano, fue validada en dos vías; de una parte con la implementación de una integración con una entidad real que gestiona datos personales y de otra parte con la opinión de la autoridad en protección de datos en Colombia. A continuación se presentan los detalles de estas validaciones.

6.1. Validación de la solución informática S1581 con una entidad real

El objetivo de la validación con una entidad real es poder tener un escenario en el cual la solución informática interactúe con una base de datos real y así establecer la flexibilidad de los mecanismos de integración e identificar los posibles obstáculos o elementos no contemplados sobre la solución. De igual manera poder tener retroalimentación desde el punto de vista de una entidad sobre la solución.

La Pontificia Universidad Javeriana fue la entidad con la cual se realizó el proceso de validación de la solución. Para el ejercicio académico de este proyecto la entidad permitió el acceso a un ambiente de pruebas de su sistema principal ERP, este sistema soporta y gestiona los procesos académicos y administrativos de la entidad. En este documento se omiten algunos detalles técnicos de la integración, por consideraciones de confidencialidad con la entidad.

La entidad trata datos personales de estudiantes, egresados, empleados y profesores; principalmente cuenta con información de tipo personal en las categorías de datos biográficos, académicos y laborales. Las actividades realizadas involucraron la clasificación de los datos personales, el diseño del servicio de información, análisis de mecanismos de integración y la construcción del servicio de información. La Figura 21 presenta la consulta de datos personales realizada a la Pontificia Universidad Javeriana para un ciudadano que ha tenido vinculaciones con esta entidad como estudiante, empleado y profesor; la imagen presenta la clasificación de datos extraída del sistema y la visualización de datos de identificación mediante la opción de navegación taxonómica.

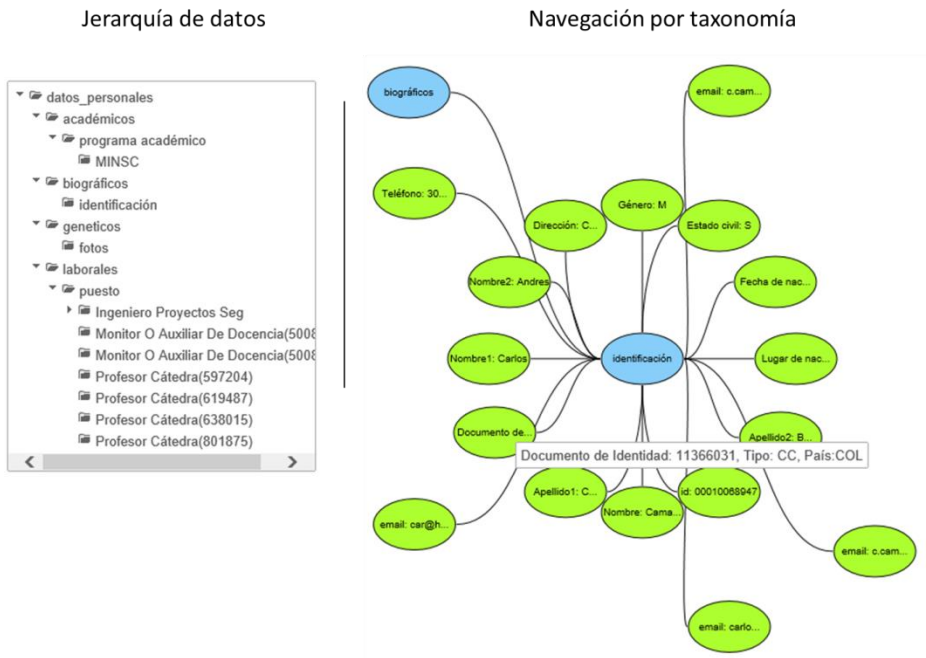

Figura 21. Consulta de datos personales a la Pontificia Universidad Javeriana

Como resultados se obtuvo que la solución S1581 logró integrar rápidamente el servicio implementado para la Pontificia Universidad Javeriana, el servicio de información fue desarrollado en un periodo corto, alrededor de 20 días; de este trabajo se obtuvieron varias experiencias y oportunidades de mejora para la Solución informática S1581, tales como:

- El proceso en las empresas para lograr la autorización y concretar que se realice una iniciativa de este tipo puede ser largo, se requiere concientización por parte de la alta dirección y en particular de los responsables directos de los datos personales.
- Las entidades pueden contar con información personal que aún no se ha identificado, lo que podría generar consultas incompletas. Sin embargo, se observa que la solución propuesta ofrece flexibilidad para que la entidad pueda actualizar y mejorar el servicio sin requerir cambios en la solución.
- Aunque este trabajo entrega pautas para la clasificación de datos personales, las entidades son responsables de esta tarea. El éxito de la clasificación estará dado por el entendimiento que tenga la entidad de los datos personales que gestiona.
- Para ciertos datos, como los de tipo laboral por ejemplo, es difícil establecer la frontera de hasta donde el ciudadano es el titular y cuando se trata de información propia de la entidad.
- Desde el punto de vista técnico se identifica como oportunidad de mejora incluir nativamente el manejo de tipos de datos estructurados como lo puede ser un contrato o la vinculación a un programa académico.
- Otra oportunidad se refleja en la mejora del trato de datos multí-valor, ya que actualmente se ven como datos diferentes o deben ser formateados por las entidades para verse como un solo valor.

- Mejorar el manejo de formatos, por ejemplo los tipos de datos fecha son formateados por la entidad, esto puede confundir a los ciudadanos al revisar diferentes entidades.

6.2. Validación de la solución informática S1581 con la Superintendencia de industria y comercio

Se realizó una validación del proyecto y sus resultados con la Superintendencia de Industria y Comercio, autoridad colombiana en materia de protección de datos, a través de la Dirección de investigación de protección de datos personales. El objetivo fue evaluar la solución S1581: Solución Informática de Gestión de Datos Personales del Ciudadano Colombiano en aspectos tales como pertinencia, utilidad e impacto y validar el alcance del proyecto, las oportunidades de implementación, impactos potenciales y la posible aceptación por parte de los actores involucrados (ciudadanos y entidades).

La validación se realizó mediante entrevistas realizadas en el mes de diciembre de 2013 y la aplicación de un cuestionario desarrollado como instrumento para este fin. En esta validación participaron los funcionarios: Carlos Enrique Salazar Muñoz, Director de investigación de protección de datos personales y Aida Lucia Hurtado Bejarano, Ingeniera de esta misma entidad (ver Anexo 5).

La solución informática tuvo una buena aceptación como iniciativa para facilitar a los ciudadanos ejercer sus derechos; los entrevistados resaltaron los elementos de seguridad tenidos en cuenta y la facilidad de uso de la herramienta. Consideran que la solución informática S1581 facilita al ciudadano la gestión de sus datos personales y aporta a las entidades en el cumplimiento de la ley 1581 de 2012.

De la solución informática tres funcionalidades se identificaron como las de mayor utilidad y se relacionan a continuación:

- Consulta de entidades responsables de los datos personales del ciudadano
- Consulta del detalle de datos personales del ciudadano.
- Registro de solicitudes de rectificación de datos personales.

De igual manera indicaron que una solución de este tipo genera un nivel de responsabilidad muy alto, ya que algún defecto o falencia en aspectos tales como la autenticación y privacidad del ciudadano conllevarían a incurrir en faltas graves contra la ley. De otra parte hicieron énfasis en que en una implementación nacional se pueden encontrar barreras como la falta de voluntad de las entidades para acoger la solución y la necesidad de posibles reformas a la ley para hacerla valida, obligar a las entidades a utilizarla y conferir la responsabilidad de dicha solución a un ente público como la Superintendencia de Industria y Comercio.

Como oportunidades de mejora indican que es posible afinar el control de las solicitudes de los titulares incluyendo elementos de seguimiento y revisión de estado. Así mismo indican que sería conveniente incluir otros mecanismos de autenticación que, sin sacrificar seguridad, permitan dar mayor acceso a titulares que no cuenten con certificados digitales.

Como sugerencia resaltan la importancia de aclarar a los titulares de los datos personales, que la solución informática brinda un acceso limitado a los datos y que nunca se tendrá una certeza total de dónde está su información. Los consultados perciben que la solución puede ser ampliamente aceptada por las entidades para una implementación local, que les permitiría sobrepasar retos como la integración de sus sistemas y así agilizar el cumplimiento de la ley.

7. Resultados obtenidos

Como resultados obtenidos se resalta los siguientes:

a. Generación de taxonomía de datos personales, como orientación para la clasificación por parte de las entidades.
b. Implementación de la Solución Informática S158: SOLUCIÓN INFORMÁTICA DE GESTIÓN DE DATOS PERSONALES DEL CIUDADANO COLOMBIANO, la cual presenta los siguientes beneficios:
   - Facilitar al ciudadano la gestión de sus datos personales en acuerdo a la ley 1581 de 2012.
   - Aportar a las entidades en el cumplimiento de la ley 1581 de 2012.
   - Permitir la identificación de entidades que tiene los datos personales del ciudadano.
   - Centralizar y unificar los procesos de consulta y rectificación de datos personales.
c. Creación de proveedores de autenticación implementados con tecnología OpenID. Estos proveedores podrían ser utilizados por otras iniciativas de *e-goverment* , que requieran autenticación del ciudadano.
d. Diseño e implementación de mecanismo multinivel de autenticación.
e. Creación de solución orientada por los principios de Privacidad por Diseño (Privacy by Design - PbD), algunos de los elementos tenidos en cuenta son:
   - Diseño e implementación de mecanismos de autenticación del ciudadano.
   - Diseño e implementación de mecanismos de autenticación mutua entre los componentes de la solución, utilizando certificados digitales.
   - Cifrado de datos mediante protocolo https para acceso del ciudadano y comunicación entre componentes.

     Invocación en tiempo real de servicios de información, evita el almacenamiento de los datos personales en la base de datos local; asegurando que los datos personales son presentados únicamente al titular.

V - CONCLUSIONES Y TRABAJOS FUTUROS

8. Conclusiones

La creación de la solución S1581 presenta una solución novedosa que promueve y aprovecha los esfuerzos particulares de cada entidad para lograr una solución unificada y orientada al ciudadano. Pretende empoderar al ciudadano para que sea él quien controle sus datos personales ejerciendo su derecho de Autodeterminación Informativa y de Habeas Data; así mismo concientizarlo para adoptar una actitud activa donde se preocupe por interrogantes como: ¿Quién tiene sus datos personales?, ¿Dónde están dichos datos?, ¿Son correctos?, etc.

El desarrollo del proyecto, contempla dos frentes en los cuales se prevé un aporte significativo. Por una parte, sí el Estado establece una plataforma como S1581, facilitará a los ciudadanos el acceso a la información, reducirá las necesidades de capacitación y disminuirá los tiempos requeridos para gestionar la información personal, lo cual beneficiará al ciudadano. La solución informática puede ser implementada en otros países que quieran apoyar sus políticas de protección de datos con el uso de TICs.

Por otra parte, si las entidades apropian esta tecnología se verán favorecidas con la implantación de un producto que desde su concepción vincula los principios de "Privacy by design" y de protección de datos personales. Así mismo, la entidad que desarrolle la interfaz de integración podrá cumplir rápidamente con algunos de los deberes establecidos en la ley 1581 de 2012 que son exigidos desde abril de 2013 y así evitar posibles sanciones. A futuro la plataforma podrá complementarse con actividades consultivas que ayuden en la implementación de la ley.

Una solución informática como S1581 podría estar a cargo de un ente de vigilancia como la Superintendencia de Industria y Comercio, sin embargo para que la entidad pueda asumir esta responsabilidad se requiere que la ley indique estas funciones. Dado que la ley 1581 es de tipo estatutaria su modificación es compleja, esto dificulta el tener un sponsor que promueva la implementación de la solución con un alcance nacional.

De acuerdo a la validación se observa que uno de los mayores obstáculos de la implementación de la solución informática a nivel nacional es la falta de voluntad y de interés por parte de las entidades para generar servicios de información para ser consultados desde un sistema externo. Sin embargo, la implementación de la solución informática en un ambiente local cobra mayor relevancia para las entidades dado que permitiría integrar sus aplicaciones para mostrar al ciudadano una sola vista de gestión de datos personales.

La solución informática puede tomarse como punto de partida para la implementación de otros servicios masivos apoyados por TICs que estén enfocados al ciudadano, teniendo en cuenta características como: mecanismos de autenticación para el ciudadano, autenticación multinivel, uso de servicios web con tecnología hibrida SOAP + JSON, estrategias de cifrado y seguridad, empleo de tecnologías como JEE6, etc.

9. Trabajos Futuros

La solución informática presenta un catálogo general de tipos de datos personales, que puede orientar sobre cómo clasificar la información personal y puede establecerse como un lenguaje común para el intercambio o tratamiento de este tipo de datos. Algunos proyectos que se pueden abordar desde ámbito son:

- Seguir ampliando el banco de tipos de datos y ajustar las categorías de acuerdo a lo que pueda solicitar el Registro Nacional de Bases de Datos.
- Realizar un estudio que permita profundizar sobre la taxonomía de datos personales. en este estudio se puede analizar bases de datos de entidades de diferentes sectores y establecer patrones de clasificación.
- Generar una metodología que puedan seguir las entidades para realizar la clasificación de sus datos personales.
- Generar un sistema inteligente que sea capaz de analizar una base de datos para identificar los datos personales y sugerir su clasificación bajo los parámetros establecidos en la taxonomía. Este sistema podría distinguir los datos de tipo sensible y generar notificaciones al respecto.
- Puede incluirse en la solución informática un componente de clasificación en tiempo real que muestra al ciudadano sus datos por categorías aun cuando la entidad no los haya clasificado.

La solución informática pueden complementarse con funcionalidades tales como:

- Optimización de la solución en el mecanismo de búsqueda asincrónica de entidades, teniendo en cuenta una gran cantidad de entidades, altos volúmenes de transacciones por parte de los ciudadanos y finalmente altos volúmenes de datos en los sistemas a consultar.
- Componente de análisis de datos personales del ciudadano que permita evaluar el nivel de riesgo de tener información en determinada entidad.
- Generación de correlación de datos entre entidades que permitan saber dónde la información puede estar incompleta o ser inexacta.
- Revisión proactiva y automática de datos personales, que permita notificar al ciudadano cuando se identifique una nueva entidad que recolecte su información personal.
- Desarrollo de componente de búsqueda de responsable de datos personales por internet, enfocado al análisis de redes sociales y repositorios que publican información online estructurada o no estructurada.
- Desarrollo de versión para dispositivos móviles e inteligentes. Por ejemplo para la construcción de módulos de consulta similares a un cajero automático.

Desde el punto de vista de autenticación e identificación del ciudadano se visualizan algunos proyectos potenciales como:

- Evaluación de impacto, cobertura y facilidad de implementación de mecanismos de autenticación del ciudadano.
- Análisis de factibilidad de implementación de tarjetas inteligente eID como documento de identificación.
- Construcción o implementación por parte del estado colombiano de soluciones concretas de autenticación del ciudadano.

VI - REFERENCIAS

[1] Carlos G. GREGORIO, "PROTECCIÓN DE DATOS PERSONALES: EUROPA VS. ESTADOS UNIDOS, TODO UN DILEMA PARA AMÉRICA LATINA," *Transparentar al Estado: la Experiencia Mexicana de Acceso a la Información*, 2004 [Online]. Available: http://biblio.juridicas.unam.mx/libros/libro.htm?l=1407

[2] Colombia, *Constitución Política*. 1991 [Online]. Available: http://web.presidencia.gov.co/constitucion/index.pdf

[3] Congreso de Colombia, *Ley Estatutaria 1581 de 2012*. 2012 [Online]. Available: www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981

[4] Ministerio de Comercio, Industria y Turismo, *Decreto 1377 de 2013*. 2013 [Online]. Available: https://www.mincomercio.gov.co/descargar.php?id=65007

[5] Oracle America, Inc., "The Java EE 6 Tutorial." [Online]. Available: http://docs.oracle.com/javaee/6/tutorial/doc/bnayl.html. [Accessed: 10-Aug-2013]

[6] Oracle, "MySql." [Online]. Available: http://www.mysql.com/

[7] json.org, "Introducing JSON." [Online]. Available: http://www.json.org/. [Accessed: 11-Aug-2013]

[8] M. Stamp, *Information security principles and practice*. Hoboken, N.J.: Wiley, 2011 [Online]. Available: http://www.ietf.org/rfc/rfc3280.txt

[9] "OpenID." [Online]. Available: http://openid.net/

[10] Oracle America, Inc., "JAX-WS Reference Implementation (RI) Project." [Online]. Available: http://jax-ws.java.net/

[11] JBoss Community, "JBoss Application Server." [Online]. Available: http://www.jboss.org/jbossas/

[12] Agencia Española de Protección de Datos (AEPD), "El director de la AEPD destaca que la protección de datos contribuye a generar confianza en las nuevas tecnología," 28-Jan-2013.

[13] Jeimy J. Cano, Ph.D, CFE, "La privacidad de los datos: un reto empresarial técnico/jurídico," *Revista sistemas*, pp. 88–92, Apr-2012.

[14] Congreso de Colombia, *Ley Estatutaria 1266 de 2008*. 2008 [Online]. Available: http://www.secretariasenado.gov.co/senado/basedoc/ley/2008/ley_1266_2008.html

[15] Rafael Hernando Gamboa Bernate, "Seguridad y privacidad o seguridad vs. privacidad, ¿compatibles?," *Revista sistemas*, pp. 10–15, Apr-2012.

[16] Ann Cavoukian, Ph.D., "Privacy by Design - Los 7 Principios Fundamentales." [Online]. Available: http://viepriveeintegree.ca/content/uploads/2009/08/7foundationalprinciples-spanish.pdf

[17] Information Commissioner's Office (ico.), "Privacy by design," 28-Jan-2013. [Online]. Available: http://www.ico.gov.uk/for_organisations/data_protection/topic_guides/privacy_by_design.aspx. [Accessed: 09-Feb-2013]

[18] Asociación Colombiana de Ingeniería de Sistemas - ACIS, "Seguridad vs. privacidad," *Revista sistemas*, pp. 50–67, Apr-2012.

[19] K. Beck, *Extreme Programming Explained: Embrace Change*, US ed. Addison-Wesley Professional, 1999.

[20] Don Wells, "Extreme Programming Project." [Online]. Available: http://www.extremeprogramming.org/map/project.html. [Accessed: 03-Feb-2013]

[21] M. Cohn, *User Stories Applied: For Agile Software Development*, 1st ed. Addison-Wesley Professional, 2004.

[22] "Hábeas data y derecho a la privacidad," *El Derecho*, vol. 161–866.

[23] Agencia Española de Protección de, "Resolución de Madrid - Estándares Internacionales sobre Protección de Datos Personales yPrivacidad," presented at the 31 Conferencia Internacional de Autoridades de Protección de Datos y Privacidad, Madrid España, 2009.

[24] National Institute of Standards and Technology (NIST), "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)." Apr-2012 [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf

[25] GAO - United States Government Accountability Office, "GAO Report 08-536, Privacy: Alternatives Exist for Enhancing Protection of Personally Identifiable Information." GAO, May-2008 [Online]. Available: http://www.gao.gov/new.items/d08536.pdf

[26] M. Masciotra, *El habeas data la garantiÌ • a polifuncional*. La Plata: Platense, 2.

[27] "Declaración Universal de Derechos Humanos." [Online]. Available: http://www.un.org/es/documents/udhr/index.shtml. [Accessed: 28-Dec-2013]

[28] European Court of Human Rights, Council of Europe, "Convenio europeo de derechos humanos revisado en conformidad con el Protocolo n° 11." 2010 [Online]. Available: http://www.echr.coe.int/Documents/Convention_SPA.pdf

[29] "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data," 15-Jul-2013. [Online]. Available: http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm. [Accessed: 15-Jul-2013]

[30] Consejo de Europa, "Convenio 108 del Consejo de Europa." 28-Jan-1981 [Online]. Available: http://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/Convenio108-19811.pdf

[31] A. I. H. Ortíz, *El derecho a la intimidad en la nueva ley orgánica de protección de datos personales*. Librería-Editorial Dykinson, 2002.

[32] Parlamento Europeo y del Consejo, "Directiva 95/46/CE." Diario Oficial de las Comunidades Europeas, 24-Oct-1995.

[33] Parlamento, Consejo y Comisión Europea, *CARTA DE LOS DERECHOS FUNDAMENTALES DE LA UNIÓN EUROPEA*. 2010 [Online]. Available: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0389:0403:ES:PDF

[34] España, *Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal (LORTAD)*. 1992.

[35] España, *Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.* 1999 [Online]. Available: http://www.boe.es/boe/dias/1999/12/14/pdfs/A43088-43099.pdf

[36] Agencia Española de Protección de Datos, "Nota de prensa: Durante la inauguración de la Jornada '20 años de protección de datos en España' El director de la AEPD destaca que la protección de datos contribuye a generar confianza en las nuevas tecnologías," Madrid, España, Jan. 2013.

[37] *PROPUESTA REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos)*. 2012.

[38] COOLEY, TH. M., "A Treatise on the Law of Torts or the Wrongs Which Arise Independently of Contract." Callaghan, 1879.

[39] Warren,Brandeis, "The Right to Privacy." Harvard Law Review, 15-Dec-1985 [Online]. Available: http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html

[40] "Pierce v. Society of Sisters - 268 U.S. 510 (1925)," *Justia US Supreme Court Center*. [Online]. Available: http://supreme.justia.com/cases/federal/us/268/510/case.html. [Accessed: 18-Jan-2014]

[41] "Griswold v. Connecticut - 381 U.S. 479 (1965)," *Justia US Supreme Court Center*. [Online]. Available: http://supreme.justia.com/cases/federal/us/381/479/. [Accessed: 18-Jan-2014]

[42] "Roe v. Wade - 410 U.S. 113 (1973)," *Justia US Supreme Court Center*. [Online]. Available: http://supreme.justia.com/cases/federal/us/410/113/. [Accessed: 18-Jan-2014]

[43] MARÍA NIEVES SALDAÑA, "EL DERECHO A LA PRIVACIDAD EN LOS ESTADOS UNIDOS: APROXIMACIÓN DIACRÓNICA A LOS INTERESES CONSTITUCIONALES EN JUEGO," *Teoría y Realidad Constitucional*, vol. 22, pp. 279–312, 2011.

[44] *THE PRIVACY ACT*. 1974 [Online]. Available: http://www.justice.gov/opcl/privstat.htm

[45] Nelson Remolina Angarita, "Latinoamérica y protección de datos personales en cifras (1985-2012)." 2012.

[46] Superintendencia de Industria y Comercio, "Primer Congreso Internacional De Protección De Datos (Memorias)." Jun-2013.

[47] Congreso de Colombia, *Ley 23 de 1981 - Normas sobre Ética Médica*. 1981 [Online]. Available: http://juriscol.banrep.gov.co/contenidos.dll/Normas/Leyes/1981/ley_23_1981

[48] Congreso de Colombia, *Ley 96 de 1985*. 1985 [Online]. Available: http://www.registraduria.gov.co/IMG/pdf/ley_96_1985.pdf

[49] Congreso de Colombia, *Ley 270 de 1996 - Ley estatutaria de la administración de justicia*. [Online]. Available: http://www.secretariasenado.gov.co/senado/basedoc/ley/1996/ley_0270_1996.html

[50] Congreso de Colombia, *Ley 527 de 1999 - Ley de Comercio Electrónico*. 1999 [Online]. Available: http://www.secretariasenado.gov.co/senado/basedoc/ley/1999/ley_0527_1999.html

[51] *Ley 1273 de 2009 - Ley de Delitos Informáticos*. .

[52] Corte Constitucional de Colombia, "Sentencia C-540/12 - Proyecto de ley estatutaria de fortalecimiento del marco jurídico para el desarrollo de las actividades de inteligencia y contrainteligencia." 2011.

[53] Nelson Remolina Angarita, "¿TIENE COLOMBIA UN NIVEL ADECUADO DE PROTECCIÓN DE DATOS PERSONALES A LA LUZ DEL ESTÁNDAR EUROPEO?," *Rev. Colomb. Derecho Int.*, pp. 489–524, 2010.

[54] AGESIC - Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento, "Gran paso: Uruguay logra adecuación en Protección de datos," Uruguay, 2012 [Online]. Available: http://www.agesic.gub.uy/innovaportal/v/2303/1/agesic/gran_paso:_uruguay_logra_adecuacion_en_proteccion_de_datos.html

[55] Parlamento Europeo, "DECISIÓN DE EJECUCIÓN DE LA COMISIÓN de 21 de agosto de 2012," *Diario Oficial de la Unión Europea*, 21-Aug-2012.

[56] D. A. Ashbaugh, *Security software development assessing and managing security risks*. Boca Raton: CRC Press, 2009.

[57] International Privacy Commissioners and and Data Protection Authorities, "Privacy by Design, Strong Privacy Protection – Now, and Well into the Future," presented at the 33rd International Conference of Data Protection and Privacy Commissioners, 2011 [Online]. Available: www.privacybydesign.ca

[58] UNIÓN INTERNACIONAL DE TELECOMUNICACIONES, "Arquitectura de seguridad para sistemas de comunicaciones extremo a extremo," *SERIE X: REDES DE DATOS Y COMUNICACIÓN ENTRE SISTEMAS ABIERTOS Seguridad*, vol. UIT-T X.805 SECTOR DE NORMALIZACIÓN DE LAS TELECOMUNICACIONES DE LA UIT, Oct-2003.

[59] H. F. Tipton and M. Krause, *Information Security Management Handbook, Fifth Edition*, 5th ed. Auerbach Publications, 2003.

[60] W. Rankl and W. Effing, *Smart Card Handbook*. John Wiley & Sons, 2010.

[61] W. Rankl, *Smart Card Applications: Design models for using and programming smart cards*. John Wiley & Sons, 2007.

[62] Smart Card Alliance, "Acceso Lógico Seguro: El Papel de las Tarjetas Inteligentes en una Autenticación Más Sólida." Oct-2004 [Online]. Available: http://www.smartcardalliance.org/latinamerica/translations/Logical_Access_Security_Spanish.pdf

[63] D. Todorov, *Mechanics of User Identification and Authentication: Fundamentals of Identity Management*. CRC Press, 2012.

[64] Telecommunication Standardization Sector (ITU-T), "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile." Network Working Group, Apr-2012 [Online]. Available: http://www.ietf.org/rfc/rfc3280.txt

[65] OpenID Foundation and Information Card Foundation, "Open Trust Frameworks for Open Government: Enabling Citizen Involvement through Open Identity Technologies." 2009 [Online]. Available: http://openid.net/docs/Open_Trust_Frameworks_for_Govts.pdf

[66] OpenID Fundation, "OpenID Foundation website." [Online]. Available: http://openid.net/. [Accessed: 09-Jan-2014]

[67] OASIS, "OASIS Web Services Security (WSS) TC." [Online]. Available: https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wss

[68] OpenID Fundation, "Government | OpenID." [Online]. Available: http://openid.net/government/. [Accessed: 09-Jan-2014]

[69] United Nations, "United Nations E-Government Survey 2012." 2012 [Online]. Available: http://unpan1.un.org/intradoc/groups/public/documents/un/unpan048065.pdf

[70] Ministerio Español de Política Territorial y Administración and Capgemini Consulting, "Estudio sobre Mejores Prácticas en Gobierno Electrónico en Europa." Dec-2010.

[71] E. Soares, "Global Legal Monitor: Brazil: New National ID Card Launched | Global Legal Monitor | Law Library of Congress | Library of Congress," 04-Jan-2011. [Online]. Available: http://www.loc.gov/lawweb/servlet/lloc_news?disp3_l205402458_text. [Accessed: 08-Jan-2014]

[72] RENIEC - Registro Nacional de Ientificación y Estado Civil, "DNI Electrónico - Perú." [Online]. Available: http://www.reniec.gob.pe/portal/acercaDni.htm#

[73] Adriana Rivera, "'Chip cubano' prolifera en América Latina," *El Nacional I El Universal*, Mexico, 08-Mar-2013 [Online]. Available: http://www.eluniversal.com.mx/el-mundo/2013/-34chip-cubano-34-prolifera-en-america-latina-940042.html

[74] "Portal portal de identidad (Personalausweis portal)." [Online]. Available: http://www.personalausweisportal.de/DE/Home/home_node.html

[75] Bélgica, "eID: Carte d'identité électronique." 2013 [Online]. Available: http://eid.belgium.be/en/

[76] Dinamarca, "Ciudadano (borger)." [Online]. Available: https://www.borger.dk/Sider/default.aspx

[77] Bélgica, "my.belgium." [Online]. Available: http://my.belgium.be/

[78] Holanda, "Mi Gobierno (MijnOverheid)." [Online]. Available: https://mijn.overheid.nl

[79] *Java EE 6 Pocket Guide*. [Online]. Available: http://shop.oreilly.com/product/0636920026464.do. [Accessed: 22-Jan-2014]

[80] A. Goncalves and J. Farley, *Beginning Java EE 6 platform with GlassFish 3 from novice to professional*. [New York]: Apress, 2010.

[81] B. Upadhyaya, Y. Zou, H. Xiao, J. Ng, and A. Lau, "Migration of SOAP-based services to RESTful services," in *2011 13th IEEE International Symposium on Web Systems Evolution (WSE)*, 2011, pp. 105–114.

[82] "RESTful Web services: The basics," 06-Nov-2008. [Online]. Available: http://www.ibm.com/developerworks/webservices/library/ws-restful/. [Accessed: 11-Aug-2013]

[83] G. Serme, A. S. de Oliveira, J. Massiera, and Y. Roudier, "Enabling Message Security for RESTful Services," in *2012 IEEE 19th International Conference on Web Services (ICWS)*, 2012, pp. 114–121.

[84] Kelvin Lawrence, IBM and Chris Kaler, Microsoft, "Web Services Security: SOAP Message Security 1.1." [Online]. Available: https://www.oasis-open.org/committees/download.php/16790/wss-v1.1-spec-os-SOAPMessageSecurity.pdf

[85] JBoss Community, "Seam." [Online]. Available: http://www.seamframework.org/Seam2

[86] JBoss Community, "JBoss Developer Framework." .

[87] "The Future Of JBoss Seam And Apache DeltaSpike." [Online]. Available: http://www.infoq.com/news/2012/04/seam-deltaspike. [Accessed: 04-Aug-2013]

[88] JBoss Community, "JBoss Forge Site." [Online]. Available: http://forge.jboss.org/index.html

[89] Oracle, "Oracle WebLogic Server." [Online]. Available: http://www.oracle.com/technetwork/middleware/weblogic/overview/index.html?ssSourceSiteId=ocomen

[90] IBM, "IBM WebSphere Application Server." [Online]. Available: http://www-03.ibm.com/software/products/es/appserv-was/

[91] json-schema.org, "JSON Schema." [Online]. Available: http://json-schema.org/

[92] Kent Beck, "Manifesto for Agile Software Development." 2001 [Online]. Available: http://agilemanifesto.org/

[93] M. Cohn, *Succeeding with agile: software development using Scrum*. Upper Saddle River, NJ: Addison-Wesley, 2010.

[94] K. S. Rubin, *Essential Scrum: a practical guide to the most popular agile process*. Upper Saddle River, NJ: Addison-Wesley, 2013.

[95] W. C. Wake, *Extreme Programming Explored*, 1st ed. Addison-Wesley Professional, 2001.

[96] Instituto Federal de Acceso a la Información y Protección de Datos, "Sistema Persona." [Online]. Available: http://persona.ifai.org.mx/persona/welcome.do. [Accessed: 07-Jun-2013]

[97] G. IWI, *Ley orgánica de protección de datos de carácter personal*. Editorial Vértice, 2009.

[98] Superintendencia de Industria y Comercio, "Portal Superintendencia de Industria y Comercio, sección Protección de datos personales." [Online]. Available: http://www.sic.gov.co/es/proteccion-de-datos-personales;jsessionid=V0nwes3LQjdHai4-dO2LQM0N.undefined. [Accessed: 03-Feb-2013]

[99] Agencia Española de Protección de Datos (AEPD), "El derecho fundamental a la protección de datos: Guía para el Ciudadano." AEPD [Online]. Available: http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/GUIA_CIUDADANO_OK.pdf

[100] A. P. Sage and W. B. Rouse, *Handbook of Systems Engineering and Management*. John Wiley & Sons, 2011.

[101] Bill Phifer, "DAR Basics: Applying Decision Analysis and Resolution in the Real World." EDS, 10-Apr-2013 [Online]. Available: http://www.sei.cmu.edu/library/assets/dar.pdf

[102] H. O. B. R. Oscar Almanza Rodríguez, "Entrevista a funcionarios Coordinación de Diseño e Innovación de Gobierno en línea, Ministerio de Tecnologías de la Información y las Comunicaciones.," 24-Apr-2013.

[103] "Nuestros servicios, Liderar y soportar la estrategia de Gobierno en línea," *Gobierno en línea*. [Online]. Available: http://programa.gobiernoenlinea.gov.co/nuestros-servicios.shtml?apc=b-x;x;x;x1-&x=124

[104] J. C. M. C. Jose Ricardo Aponte Oviedo, "Entrevista a funcionarios plataforma de Interoperabilidad y seguridad de Gobierno en línea, Ministerio de Tecnologías de la Información y las Comunicaciones.," 26-Apr-2013.

[105] Gobierno en línea, "Tramitador en línea." [Online]. Available: http://www.intranet.gov.co/index.php?option=com_content&task=view&id=278&Itemid=503

[106] "OpenID Authentication 2.0 - Final," 05-Dec-2007. [Online]. Available: http://openid.net/specs/openid-authentication-2_0.html

[107] OpenID for Java Project Team, "OpenId for Java." [Online]. Available: https://code.google.com/p/openid4java/

[108] J. B. D. Hardt, "OpenID Attribute Exchange 1.0 - Final." 05-Dec-2007 [Online]. Available: http://openid.net/specs/openid-attribute-exchange-1_0.html

[109] Google team, "Federated Login for Google Account Users." [Online]. Available: https://developers.google.com/accounts/docs/OpenID

[110] "Eclipse - The Eclipse Foundation open source community website." [Online]. Available: http://www.eclipse.org/. [Accessed: 19-Jan-2014]

[111] Víctor Manuel Toro and María Consuelo Franky, "Toma de decisiones en la empresa sobre Tecnologías de Información," Jun-2013.

VII - GLOSARIO

Autorización: *Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales*[3].

Base de datos: *Conjunto organizado de datos personales que sea objeto de Tratamiento*[3].

Ciudadano colombiano: Se considerara ciudadano, al natural de Colombia, colombiano, que haya adquirido la ciudadanía, de acuerdo a la constitución "la ciudadanía se ejercerá a partir de los dieciocho años" [2].

Dato personal: *Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables*[3].

Dato sensible: Datos referidos a cuestiones íntimas de las personas, tales como religión, raza, ideología, opinión política, posición filosófica, tendencias psicológicas, relaciones sexuales, situaciones familiares y parentales, etc.[26]

Delegatura para la Protección de Datos Personales: Unidad de la Superintendencia de Industria y Comercio encargada de garantizar que en el tratamiento de datos personales se respeten los principios, derechos, garantías y procedimientos previstos en la ley 1581 de 2012[3].

Encargado del Tratamiento: *Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento*[3].

Finalidad: Fin con que o por que se ha recolectado la información personal.

Responsable del Tratamiento: *Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos*[3].

SIC: Abreviatura de Superintendencia de Industria y Comercio.

Superintendencia de Industria y Comercio: Autoridad en materia de protección de datos personales, mediante la "Delegatura para la Protección de Datos Personales"[3, p. 15], vigila el cumplimiento de la Ley 1581 de 2012.

Titular: *Persona natural cuyos datos personales sean objeto de Tratamiento*[3].

Tratamiento: *Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión*[3].

VIII - ANEXOS

Anexo 1. Descripción Historias de Usuario

Lista las Historias de Usuario(HU) que fueron identificadas como candidatas para ser implementadas en la solución S1581. Por cada Historia de Usuario se incluye id, Fuente, descripción, justificación, clasificación FURPS+ , actor y nivel de riesgo. También se incluye tabla descriptiva de las fuentes de donde se extrajo la HU.

Anexo 2. Evaluación de historias de usuario.

En este anexo se definen los requerimientos funcionales, plasmados como historias de usuario, que fueron implementados en la solución informática S1581; la selección de estas funcionalidades se realizó mediante el proceso de Análisis y Resolución de Decisiones (DAR)[101][111]. Este anexo incluye la explicación de la metodología Análisis y Resolución de Decisiones (DAR) utilizada, y la evaluación de las historias de usuario.

Anexo 3. Taxonomía de datos personales

Presenta la clasificación de datos personales realizada mediante la taxonomía planteada en este trabajo. Para la realización de esta taxonomía se han tenido en cuenta los tipos de datos personales plasmados en la ley colombiana de protección de datos[3], la directiva europea 95/46/CE[32], las clasificaciones que algunas entidades han realizado de los datos personales como el "sistema personas" a cargo del "Instituto Federal de Acceso a la Información y Protección de Datos" (IFAI)[96], Agencia Española de Protección de Datos[97] y aporte propio del autor.

Anexo 4. Código fuente de solución informática

En este anexo se encuentra el código fuente de la solución informática. Se puede descargar los 6 proyectos eclipse que hacen parte de la solución y los correspondientes archivos de despliegue (*.war).

Anexo 5. Cuestionario de Validación con Superintendencia de Industria y Comercio.

Este anexo representa el cuestionario que fue diligenciado por funcionarios de la Superintendencia de Industria y Comercio con el objeto de dar retroalimentación acerca de la solución informática S1581 y el desarrollo del proyecto.

Anexo 6. Cuestionario de Validación con Pontificia Universidad Javeriana.

Este anexo representa el cuestionario que fue diligenciado por funcionarios de la Pontificia Universidad Javeriana con el objeto de dar retroalimentación acerca de la solución informática S1581 y el desarrollo del proyecto.

Anexo 7. Configuración de contenedor de aplicaciones JBoss para alojar solución informática S1581

En este documento se encuentra las consideraciones y pasos a seguir para configurar el contenedor de aplicaciones JBoss para alojar solución informática S1581.

Anexo 8. Manual del usuario

En este documento se describe cómo utilizar la solución informática S1581. Se explica elementos como autenticación, búsqueda de entidades, consulta de datos personales, etc.

Anexo 9. Marco contextual completo

En este anexo se encuentra una versión del marco contextual que amplia algunos conceptos y describe elementos adicionales que han influido en la evolución de la protección de los datos personales y su marco jurídico.