Definición de un Sistema Global de Información en Materia de Discapacidad en la Universidad

Observatorio Universidad y Discapacidad

Fundación ONCE
Universitat Politècnica de Catalunya. BarcelonaTech

DEFINICIÓN DE UN SISTEMA GLOBAL DE INFORMACIÓN EN MATERIA DE DISCAPACIDAD EN LA UNIVERSIDAD

Edita: Observatorio Universidad y Discapacidad (entidad formada por Fundación ONCE y la Cátedra de Accesibilidad de la Universidad Politécnica de Cataluña-BarcelonaTech). Vilanova i la Geltrú (Barcelona). enero 2014.

ISBN obra completa: 84-695-9633-0
ISBN volumen 1: 84-695-9669-1

Libro digital en: www.catac.upc.edu

Este trabajo ha sido realizado por la Cátedra de Accesibilidad de la Universitat Politècnica de Catalunya con el apoyo financiero de la Unión Europea a través del Programa Operativo de Lucha contra la Discriminación cofinanciado por el Fondo Social Europeo. El contenido y opiniones técnicas que se consignan en este informe no vinculan ni reflejan las posiciones de la Fundación ONCE ni de ningún órgano de la Unión Europea.

UNIÓN EUROPEA
FONDO SOCIAL EUROPEO
El Fondo Social Europeo invierte en tu futuro

Fundación ONCE
para la Cooperación e Inclusión Social de Personas con Discapacidad

UNIVERSITAT POLITÈCNICA DE CATALUNYA
BARCELONATECH
Cátedra de Accesibilidad

Dirección y coordinación

Daniel Guasch Murillo

Director Cátedra de Accesibilidad, UPC

Jesús Hernández Galán

Director de Accesibilidad Universal, Fundación ONCE

Equipo investigador

Israel Martín

Francisco José Rico

Yolanda Guasch

Raquel Vállez

Maria Hortensia Álvarez

CONTENIDOS

LISTA DE TÉRMINOS

Término	Definición
Escala Barthel	Medida de capacidad individual para realizar las actividades de la vida diaria (comer, bañarse, higiene personal y caminar).
Sistema Braille	Sistema de lectura y escritura para personas con discapacidad visual basado en puntos en relieve taladrados en el papel.
Datos de carácter personal	Cualquier información concerniente a personas físicas identificadas o identificables.
Fichero	Todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.
Tratamiento de datos	Operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.
Responsable del fichero o tratamiento	Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento.
Afectado o interesado	Persona física titular de los datos que sean objeto de tratamiento.
Procedimiento de disociación	Todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable.
Encargado del tratamiento	La persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento.
Consentimiento del interesado	Toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen.

Cesión o comunicación de datos	Toda revelación de datos realizada a una persona distinta del interesado.
Fuentes accesibles al público	Aquellos ficheros cuya consulta puede ser realizada, por cualquier persona, no impedida por una norma limitativa o sin más exigencia que, en su caso, el abono de una contraprestación.

LISTA DE ACRÓNIMOS.

Acrónimo	Definición
OUD	Observatorio Universidad y Discapacidad
ONCE	Organización Nacional de Ciegos Españoles
UPC	Universidad Politécnica de Cataluña
LOPD	Ley Orgánica de Protección de Protección de Datos
AEPD	Agencia Española de Protección de Datos
UNIDISCAT	Universidad y Discapacidad en Cataluña
SIDU	Sistema de Información sobre Discapacidad en la Universidad
OGR	Órgano Gestor de la base de datos
GA	Gestor de Agregación de la base de datos
EG	Entidad Gestora
ID_{agran}	Identificador Agregado Anónimo
ID_{ps}	Identificador Pseudoaleatorio
IUA	Identificador Único de Alumno
K_{EG}	Clave AES-256 elegida de forma secreta por la Entidad Gestora. Su misión es disociar ID_{agran} de ID_{ps}.
PS	Prefijo Secreto
RAR	Repositorio de Acceso Restringido
SGBD	Sistema Gestor de Base de Datos

PRÓLOGO

A lo largo de los trabajos realizados por el Observatorio Universidad y Discapacidad se ha reflexionado sobre el entorno universitario desde múltiples puntos de vista. Visiones complementarias que intentan aportar los matices de una realidad viva y que evoluciona continuamente. Estudios cuantitativos y cualitativos llevados a cabo de forma específica para cada estudio han puesto de manifiesto la necesidad de contar con datos estadísticos reales que permitan analizar tanto una situación puntual como su evolución en el tiempo.

El estudio que se presenta a continuación aporta las reflexiones necesarias para empezar a trabajar en la consecución de un sistema de información que permita recopilar los datos estadísticos necesarios para extraer el conocimiento sobre la evolución del sistema universitario español. Demuestra la viabilidad legal, académica y técnica del sistema sin dudas ni lagunas. Aporta las especificaciones necesarias para su implementación. Y, finalmente, pone en manos de la voluntad la necesidad de su creación.

Dr. Jesús Hernández Galán
Director de Accesibilidad Universal de la Fundación ONCE.

Dr. Daniel Guasch Murillo
Director Académico de la Cátedra de Accesibilidad de la UPC-BarcelonaTech.

"Cada día sabemos más y entendemos menos."
Albert Einstein (1879-1955)

"no se puede desatar un nudo sin saber cómo está hecho."
Aristóteles (384 ac-322 ac)

"no basta saber, se debe también aplicar. No es suficiente querer, se debe también hacer."
Goethe (1749-1832)

"si me ofreciesen la sabiduría con la condición de guardarla para mí sin comunicarla a nadie, no la querría."
Séneca (2 ac-65)

EL OBSERVATORIO UNIVERSIDAD Y DISCAPACIDAD.

El Observatorio Universidad y Discapacidad (OUD) tiene la misión de estudiar y analizar todo lo relativo a la discapacidad, la accesibilidad universal, el diseño para todos y la educación inclusiva en las Universidad española. Las líneas de investigación del OUD desvelan la realidad actual de la discapacidad en el ámbito universitario. La información obtenida se analizar exhaustiva y transversalmente y con ello se consigue llegar a conclusiones que permiten ofrecer pautas, recomendaciones y guías para la consecución de la igualdad de oportunidades para las personas con discapacidad en las universidades públicas españolas.

El OUD fue creado en 2008 por la *Fundación ONCE para la cooperación e integración social de las personas con discapacidad* y la *Cátedra de Accesibilidad* de la Universidad Politécnica de Cataluña (UPC). Estas dos entidades aúnan conocimientos, experiencia y esfuerzos para desvelar la situación de las personas con discapacidad en la universidad y mejorarla.

El Observatorio estudia el estado de la accesibilidad y la discapacidad en el entorno universitario de forma periódica con lo cual analiza su evolución. En este sentido, observa globalmente aspectos como las características y requerimientos de las personas con discapacidad (considerando toda la comunidad universitaria), los servicios que la universidad les ofrece, el estado de la accesibilidad universal (en edificios, instalaciones, servicios, cursos o actividades formativas, actividades no formativas, etc.), la situación de la incorporación de los conceptos y criterios del diseño para todos o las actividades de información o sensibilización relacionadas con la accesibilidad universal.

Los estudios que el OUD lleva publicados hasta el momento son: [1]

- Accesibilidad del entorno universitario y su percepción por los estudiantes con discapacidad(2008).
- Estudio sectorial por comunidades autónomas de la accesibilidad del entorno universitario y su percepción (2009.)

[1] *Todos estos documentos están disponibles en acceso abierto en la web de la Càtedra de Accesibilidad.*

- Estudio transversal de la implantación de la accesibilidad y diseño para todos en el entorno universitario: protocolo de evaluación para la verificación de los principios de igualdad de oportunidades y accesibilidad universal en los títulos universitarios oficiales de grado (2010).
- Guía de actividades docentes para la formación en integración e igualdad de oportunidades por razón de discapacidad en las enseñanzas técnicas: accesibilidad universal y diseño para todos (2010).
- Manual para alcanzar la inclusión en el aula universitaria: pautas de accesibilidad arquitectónica, tecnológica y pedagógica para garantizar la igualdad de oportunidades en la docencia universitaria (2011.
- Guía para implementar el Universal Instructional Design (diseño Instruccional Universal) en la Universidad (2012).
- La responsabilidad social universitaria y discapacidad (RSU-D) (2012).
- Entornos adaptados para personas con discapacidad mental (2013).

En el año 2008 se llevó a cabo el primer estudio donde se comprobó el desarrollo normativo a nivel reglamentario en el que se regulan los derechos del estudiantado con discapacidad, así como la aplicación de planes de accesibilidad y la introducción de otras actuaciones concretas encaminadas a favorecer las condiciones de accesibilidad en el sector universitario. En lo referente a las percepciones del estudiantado con discapacidad ante la universidad y su accesibilidad, se consideró la dimensión físico-arquitectónica, los recursos técnicos y los servicios, así como la interacción social con los distintos actores que intervienen en esta práctica (familia, padres, profesorado).

El segundo estudio se realizó en el 2009 y extendió la metodología utilizada en el primero a las universidades públicas de Andalucía, Galicia, Extremadura, Castilla y la Mancha, Castilla y León y Comunidad Valenciana. Al ser, la accesibilidad una cuestión transversal, se analizó desde tres perspectivas diferentes: conocer la accesibilidad física y en la comunicación de la universidad, conocer los servicios y programas que ofrece la universidad respecto a la discapacidad y finalmente, conocer cómo eran percibidos ambos ámbitos por el estudiantado con discapacidad de la universidad. Los aspectos sobre la igualdad de oportunidades por razón de discapacidad recogidos en

este segundo estudio son: accesibilidad física de las instalaciones y equipos, accesibilidad de la comunicación interactiva y no interactiva, infoaccesibilidad, características del servicio de atención a la discapacidad, cuestiones docentes, relación de los compañeros, asistencia personal, inserción laboral, becas, recursos y productos de apoyo, presencia de discapacidad y/o accesibilidad en los planes de estudios.

En el 2010 se llevó a cabo el estudio *Evaluación de la implementación de los principios de igualdad de oportunidades y accesibilidad universal en los planes de estudios de los títulos de grado de las universidades españolas,* que se tradujo en una publicación con el mismo nombre en el 2011 y en diversos artículos presentados en congresos internacionales. Esta evaluación permitió conocer y evaluar el grado de implantación de los principios de igualdad de oportunidades por razón de discapacidad y de los conceptos de accesibilidad universal en los planes de estudios de titulaciones de grado de las universidades públicas españolas y formular propuestas para determinar y verificar, en mayor medida la aplicación de dichos principios.

También en el 2010 se publicó la *Guía de actividades docentes para la formación en integración de la igualdad de oportunidades por razón de discapacidad en las enseñanzas técnicas: accesibilidad*. Elaborada con un enfoque práctico y didáctico, esta guía es una herramienta de fácil uso y lectura para el profesorado de las carreras técnicas de cualquier universidad española. En ella aparecen ejemplos de aplicación de los principios de diseño para todos y criterios de accesibilidad universal en la práctica docente. Además, la aplicación de las actividades planteadas promueve la igualdad de oportunidades entre todos los estudiantes, independientemente de sus capacidades y habilidades. En definitiva esta entrega del OUD, apoya e incita la incorporación de los principios de igualdad de oportunidades mediante la realización pautada y flexible de una serie de actividades, según las necesidades formativas de cada ámbito: arquitectura, urbanismo y edificación e ingeniería y materias transversales. Al mismo tiempo que persigue que el alumnado universitario integre los valores de reconocimiento y respeto a la diversidad humana, conozca las diferentes formas de interacción de las personas con el entorno y las incorporen en su práctica profesional futura al diseñar nuevos entornos, productos o servicios.

En el 2011, se realiza el *Manual para alcanzar la inclusión en el aula universitaria: pautas de accesibilidad arquitectónica, tecnológica y pedagógica para garantizar la de oportunidades en la docencia universitaria*. Este estudio ofrece herramientas prácticas para que los profesionales de las universidades puedan poner en práctica los principios IO de una forma efectiva. En este caso la investigación se centra en el aula universitaria que es

el espacio unívoco donde se imparte la docencia. El manual recoge, gracias a la mirada transversal que proporciona la accesibilidad, un cúmulo de pautas que van des del acondicionamiento material y ergonómico de una aula física, hasta las características de una aula virtual pasando por aspectos relacionados con la pedagogía y el trato personal que se ha de tener en cuenta por parte de los docentes. Por lo tanto, cuando se hace referencia a los profesionales, no solo se considera al profesorado, sino también al personal técnico (encargado de diseñar y mantener instalaciones y equipamientos o de gestionar los servicios informáticos) y al equipo directivo y gestor (responsable de una buena parte de la accesibilidad necesaria para impartir una docencia inclusiva).

En el 2012 se realizaron los estudios *Guía para implementar el Universal Instructional Design (diseño Instruccional Universal) en la Universidad* y *La responsabilidad social universitaria y discapacidad (RSU-D)*. El primero de ellos establece cuáles son las pautas para implementar o poner en práctica el Diseño Instruccional Universal (UID) en la enseñanza universitaria a partir del análisis del modelo de la University of Guelph (Canadá). Delimita el concepto teórico de este proceso, determina el estado de la cuestión del UID en España y analiza la implementación del UID en la University of Guelph, tanto a nivel personal (implicación del personal docente) como organizativo (implicación institucional). Finalmente establece las pautas para favorecer la implementación o puesta en práctica del UID en las universidades españolas.

El segundo de los estudios del 2012, RSU-D, se centra en establecer cuáles son las pautas para implementar la Responsabilidad Social Universitaria centrada en la igualdad de oportunidades por motivo de Discapacidad (RSU-D) a partir del análisis de la RSU de las universidades españolas. El documento recoge una exposición de los objetivos de la Universidad contemporánea y de los principios de IOAU (igualdad de oportunidades y accesibilidad universal), la responsabilidad social empresarial y su aplicación en la gestión de la Universidad (RSU-D), el contexto actual de la igualdad de oportunidades por razón de discapacidad (explicitado en la RSU de las universidades que ya han incorporado esta metodología a su gestión) y finalmente la guía de implementación de la RSU-D en las universidades basada en las valoraciones anteriores.

Por último, el estudio publicado más recientemente es *Entornos adaptados para personas con discapacidad mental*. La investigación se llevó a cabo durante el 2012 y se centró en la situación de las personas con discapacidad mental en la universidad. Se determina la presencia y tipología de discapacidad mental en población universitaria. Además de llevar a cabo una primera aproximación a las necesidades genéricas del alumnado con

discapacidad mental, valorando las posibles dificultades que pueden encontrarse para la superación de los estudios universitarios y su incorporación al mercado laboral.

Como resultado se ofrecen pautas generales de actuación para con seguir que el desarrollo de los estudios universitarios de las personas con discapacidad mental se realice en un entorno óptimo.

Este ha sido el recorrido del Observatorio Universidad y Discapacidad. Las entidades que constituyen esta entidad son la Fundación ONCE y la Cátedra de Accesibilidad de la Universidad Politécnica de Catalunya.

INTRODUCCIÓN.

Según el estudio "Universidad y Discapacidad" (Fundación Universia, 2011), solo un 12% de las universidades españolas (la amplitud de la muestra es de 48 universidades) conocen con exactitud la totalidad de estudiantes con discapacidad que estudian en su universidad, el tipo de discapacidad que presentan y la rama de estudios en la que están matriculados. Este dato es francamente representativo del desconocimiento de las universidades del alumnado con discapacidad que realmente está presente en sus aulas. Conocer este hecho con exactitud es una tarea difícil pero imprescindible. Las universidades españolas están realizando considerables esfuerzos en mejorar su accesibilidad. Per enumerar algunos datos sobre ello, un 90% de las universidades evalúan sus niveles de accesibilidad teniendo planes de accesibilidad universal y diseño para todos en un 62% de los casos. Un 94% de ellas tienen a la disposición de los alumnos con discapacidad un servicio de atención especializado y un 77% cuentan con programas de apoyo a la empleabilidad e inclusión laboral del alumnado con discapacidad. Aun así queda mucho por hacer y mejorar. Pero, ¿cómo hacerlo eficazmente sin conocer el dato esencial para ello? ¿Cómo es posible establecer políticas y estrategias efectivas si no conocemos las características y necesidades de aquellas personas a las que van dirigidas?

Este proyecto ofrece una solución concisa a este problema ya que proporciona la definición técnica de un sistema que permite obtener un censo completo, riguroso y actualizado de los alumnos con discapacidad de la Universidad pública española. Este sistema queda denominado con las siglas SIDU, correspondientes a Sistema de Información sobre Discapacidad en la Universidad.

Este proyecto ofrece una solución concisa a este problema ya que proporciona la definición técnica de un sistema que permite obtener un censo completo, riguroso y actualizado de los alumnos con discapacidad de la Universidad pública española. Este sistema queda denominado con las siglas INUDIS, correspondientes a Sistema de Información sobre Discapacidad en la Universidad.

Los beneficios no son solo a nivel de la educación superior sino que sus efectos son más amplios ya que a partir de estos datos fiables y actualizados se podrán establecer sinergias muy interesantes entre las administraciones públicas, las asociaciones de personas con discapacidad, los investigadores,

las universidades y la sociedad en general en pro de la igualdad de oportunidades.

OBJETIVOS

El trabajo que se detalla a continuación tiene como objetivo principal definir un sistema global de gestión de información estadística relativa al alumnado con discapacidad en las universidades públicas españolas. Su propósito es el de facilitar a investigadores en ámbitos de discapacidad y educación superior acceder a bancos de datos estadísticos que permitan establecer modelos, tendencias y planes de actuación, mejorando así la igualdad de oportunidades de todo el alumnado. Para la consecución de este objetivo, se establecen los siguientes objetivos específicos:

Realizar un análisis sobre qué datos académicos debe gestionar el sistema. Es necesario reflexionar cuales son los datos académicos necesarios y como deben tratarse para uniformizar criterios de evaluación curricular y correlacionarlos entre sí.

Realizar un análisis legal para asegurar que el sistema cumple con los requisitos normativos necesarios en materia de protección de datos. La finalidad de la Ley de Protección de Datos Personales no debería interpretarse como una simple ocultación de la información. Más bien debe entenderse como un mecanismo que garantice el buen uso de la información y la utilización de procedimientos adecuados para ello.

Realizar un análisis técnico de un sistema de gestión de información que permita evaluar las mejores opciones que garanticen el cumplimiento de los aspectos clave tanto académicos como legales.

A partir de los análisis anteriores se deben definir las especificaciones académicas que contemplen las variables, métodos de medida y formatos necesarios para poder extraer el máximo conocimiento de los datos académicos.

Definir un protocolo de procesado de los datos académicos que garantice el cumplimiento de la ley de protección de datos. Para ello deberá describirse cómo se disocian los datos académicos de los relativos a la identidad de los alumnos, permitiendo identificar a sus propietarios de forma unívoca y anónima.

Definir la base de datos que albergará la información procedente de las universidades. Deberán priorizarse los criterios de seguridad de la información , eficiencia de su gestión, escalabilidad del sistema y su mantenimiento.

Definir los equipos, topologías de red y protocolos de comunicación necesarios para la implementación del sistema de gestión de información. Deberán incorporarse, además, criterios que garanticen la seguridad, permitan la escalabilidad del sistema, minimicen su coste económico y faciliten su mantenimiento.

Definir un sistema de uso universal, pudiéndose aplicar en todas la universidades públicas españolas, de bajo coste, priorizando software libre, y escalable, para poder incorporar necesidades futuras.

REQUERIMIENTOS INICIALES DEL SISTEMA.

Requerimientos académicos

En primer lugar, se realiza un análisis sobre los datos que debe tratar el sistema. Para ello, se parte en primer lugar, de la experiencia obtenida durante las investigaciones llevadas a cabo por el OUD, gracias a las cuales se dispone de un conocimiento exhaustivo previo de los parámetros concernientes a la igualdad de oportunidades y la accesibilidad universal en la Universidad. Las principales referencias en este sentido son los informes: Estudio sectorial por comunidades autónomas de la accesibilidad del entorno universitario y su percepción (Daniel Guasch, 2010), Evaluación de la implementación de los principios de igualdad de oportunidades y accesibilidad universal en los planes de estudios de los títulos de grado de las universidades españolas (Daniel Guasch M. H., 2012) y La responsabilidad social universitaria y discapacidad (Daniel Guasch P. D., 2013).

En segundo lugar, la Universidad Politécnica de Catalunya de la cual forma parte la Cátedra de Accesibilidad, cuenta con el conocimiento adquirido a raíz de formar parte de la Comisión Técnica de UNIDISCAT. Este proyecto está impulsado por el Consejo Interuniversitario de Cataluña que promueve la igualdad de oportunidades de los estudiantes con discapacidad, tanto en lo concerniente al acceso a las universidades de Cataluña y a la inclusión en las mismas como a la realización de los estudios universitarios, así como,

establece normas y pautas generales, comunes a todas las universidades de Cataluña, sobre los criterios para llevar a cabo las adaptaciones curriculares, las propuestas docentes y las de evaluación para todos los casos en los que fuera necesario.

A partir de este análisis los datos se han categorizado según los siguientes tipos:

- Personales.
- Académicos.
- Económicos.
- Capacidades.
- Necesidades.
- Participación.
- Calidad.

El desglose de todos ellos se muestra a continuación:

Datos personales
Nombre
Primer apellido
Segundo Apellido
NIF
NIU
Sexo
Nacionalidad
Fecha de nacimiento
Dirección
Ciudad
CP
País
Teléfono fijo
Teléfono móvil
Teléfono de emergencia

Datos personales
e-mail
Residencia habitual
Personas con quién convive
Prestaciones económicas
Actividades de ocio y tiempo libre
Actividades deportivas
Asociacionismo
Ocupación de los padres
Nivel educativo de los padres
Situación laboral de los padres
Situación laboral
Expectativas laborales

Datos académicos
Tipo de estudiante
Universidad
Facultad
Créditos matriculados
Créditos aprobados
Titulación
Tipo titulación
Créditos totales de la titulación
Curso actual
Curso de inicio
Último curso matriculado
Rama del conocimiento
Tipo de estudios
Exención de matrícula
Estudios simultáneos (1)[2]
Enseñanza simultánea (1)
Tipo de enseñanza simultánea (1)
Facultad simultánea (1)
Curso de inicio (1)
Último curso matriculado (1)

[2] En el caso de realizar más de una carrera al mismo tiempo.

Datos académicos

Estudios simultáneos (2)
Enseñanza simultánea (2)
Tipo de enseñanza simultánea (2)
Facultad simultánea (2)
Curso de inicio (2)
Último curso matriculado (2)

Datos económicos

Recibe alguna prestación económica
Recibe alguna becas
Recibe ayuda para el transporte
Recibe ayuda para financiar recursos técnicos
Recibe ayuda para financiar materiales docentes

Datos relativos a las capacidades

Discapacidad
Certificado de discapacidad
Otros documentos acreditativos
Tipo
Grado
Pronóstico de evolución
Necesita soporte en el transporte para llegar a la universidad
Necesita soporte para realizar las actividades básicas de la vida diaria
Escala Barthel
Actividades que realiza
Baremo de movilidad reducida y dificultad para hacer uso del transporte público.
Productos de soporte
Otras necesidades derivadas de la discapacidad
Medicación
Vinculación a la red pública o profesional de la salud mental
Estrategias de enfrentamiento al estrés
Otras necesidades derivadas de la discapacidad física

Datos relativos a las capacidades
Recursos técnicos para acceder a la información oral
Cuáles
Lengua de signos
Competencia en lengua de signos
Lectura labial
Competencia en lectura labial
Sistema de comunicación principal
Dificultades al hablar
Dificultades de comprensión del habla
Dificultades de orientación
Otras necesidades derivadas de la discapacidad auditiva
Tipo de discapacidad visual
Uso del Sistema Braille
Competencia en uso del Sistema Braille
Dificultades de orientación
Otras necesidades derivadas de la discapacidad visual

Datos relativos a las necesidades
Seguimiento de las clases
Seguimiento del contenido de las clases
Seguimiento de las prácticas
Realización de los exámenes
Utilización del ordenador
Acceso a la información
Ayudas técnicas
Conoce el servicio de atención a los alumnos con discapacidad
Recibe apoyo del servicio de atención a los alumnos con discapacidad
Conoce el servicio de inserción laboral
Recibe asesoramiento para su inserción laboral

Datos relativos a la participación
Participa en algún programa de movilidad
Realiza actividades deportivas realizadas en la Universidad
Realiza actividades de ocio y tiempo al aire libre en la Universidad
Realiza actividades de cooperación en la Universidad
Realiza actividades de representación estudiantil
Realiza actividades de voluntariado
Realiza prácticas de empresa

Datos para el aseguramiento de la calidad
Satisfacción sobre la accesibilidad física de la universidad
Satisfacción sobre la accesibilidad a la información de la universidad
Satisfacción sobre los servicios

Requerimientos legales

El objetivo del proyecto no es otro que el definir un sistema de información que permita recoger de forma periódica y sistemática los datos de todos los estudiantes con discapacidad de la universidad pública española. La información a tratar es de carácter personal (datos personales, de salud, necesidades, preferencias, etc.) y por lo tanto debe tratarse con el máximo rigor y confidencialidad, garantizándose en todo momento la Ley Orgánica de Protección de Datos (Gobierno de España, 1999).

Marco de referencia

A nivel del Estado español, la ley de referencia es LOPD 15/1999 de 13 de Diciembre, que a la vez se sustenta en el despliegue de la misma a través del Real Decreto 1720/2007 de 21 de Diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica de protección de datos de carácter personal actualmente en vigor.

La propia Ley, en su Título VI, artículo 35 y siguientes, define la naturaleza y régimen jurídico de la Agencia Española de Protección de Datos (AEPD), su estructura, sus funciones y sus potestades. Igualmente, en el artículo 39, regula el llamado Registro General de Protección de Datos, en el que las

organizaciones deben inscribir aquellos ficheros que contengan datos de carácter personal.

A nivel de las diferentes Comunidades Autónomas, la Ley 15/1999 ya prevé que se podrán establecer órganos de funcionamiento y transmisión de datos a la propia AEPD y cuáles son las limitaciones que existen en según que artículos de la Ley. De forma general, cabe mencionar que aquellas Comunidades Autónomas que dispongan de órganos de esta naturaleza (como por ejemplo el País Vaco, Madrid o Cataluña), gestionen básicamente registros de datos de entidades públicas donde se inscriben por ejemplo ficheros de organizaciones como ayuntamientos, universidades, colegios profesionales, etc. (Assertis, 2013)

El RD 1720/2007 se despliega en 9 Títulos y 158 Artículos:

- Título I. Disposiciones generales.
- Título II. Principios de protección de datos (constando de 3 capítulos).
- Título III. Derechos de acceso, rectificación, cancelación y oposición (constando de 4 capítulos).
- Título IV. Disposiciones aplicables a determinados ficheros de titularidad privada (constando de 2 capítulos).
- Título V. Obligaciones previas al tratamiento de datos (constando de 2 capítulos).
- Título VI. Transferencia internacional de datos (constando de 3 capítulos).
- Título VII. Código tipo.
- Título VIII. De las medidas de seguridad en el tratamiento de los datos personales (constando de 4 capítulos).
- Título IX. Procedimientos tramitados para la AEPD (constando de 7 capítulos).

Requisitos legales en el tratamiento de datos

Los datos gestionados por el sistema deben ser analizados des del punto de vista legal para asegurar el cumplimiento de la normativa vigente en lo referente a la protección de datos de carácter personal. Por ello se clasifican en base a su requerimiento de seguridad: nivel bajo, nivel medio y nivel alto.

La clasificación resultante se muestra a continuación:

Los datos gestionados por el sistema deben ser analizados des de el punto de vista legal para asegurar el cumplimiento de la normativa vigente en lo referente a la protección de datos de carácter personal. Por ello se clasifican en base a su requerimiento de seguridad: nivel bajo, nivel medio y nivel alto.

La clasificación resultante se muestra a continuación:

Nivel de seguridad bajo
Nombre
Primer apellido
Segundo Apellido
NIF
NIU
Sexo
Nacionalidad
Fecha de nacimiento
Dirección
Ciudad
CP
País
Teléfono fijo
Teléfono móvil
Teléfono de emergencia
e-mail
Residencia habitual
Personas con quién convive
Actividades de ocio y tiempo libre
Actividades deportivas
Asociacionismo
Ocupación de los padres
Nivel educativo de los padres
Situación laboral de los padres
Situación laboral
Expectativas laborales

Nivel de seguridad bajo

Tipo de estudiante
Universidad
Facultad
Créditos matriculados
Créditos aprobados
Titulación
Tipo titulación
Créditos totales de la titulación
Curso actual
Curso de inicio
Último curso matriculado
Rama del conocimiento
Tipo de estudios
Exención de matrícula
Estudios simultáneos (1)
Enseñanza simultánea (1)
Tipo de enseñanza simultánea (1)
Facultad simultánea (1)
Curso de inicio (1)
Último curso matriculado (1)
Estudios simultáneos (2)
Enseñanza simultánea (2)
Tipo de enseñanza simultánea (2)
Facultad simultánea (2)
Curso de inicio (2)
Último curso matriculado (2)
Conoce el servicio de atención a los alumnos con discapacidad
Conoce el servicio de inserción laboral
Satisfacción sobre la accesibilidad física de la universidad
Satisfacción sobre la accesibilidad a la información de la universidad
Satisfacción sobre los servicios
Participa en algún programa de movilidad
Realiza actividades deportivas realizadas en la Universidad

Nivel de seguridad bajo

Realiza actividades de ocio y tiempo al aire libre en la Universidad
Realiza actividades de cooperación en la Universidad
Realiza actividades de representación estudiantil
Realiza actividades de voluntariado
Realiza prácticas de empresa

Nivel de seguridad medio

Prestaciones económicas
Discapacidad
Necesita soporte en el transporte para llegar a la universidad
Necesita soporte para realizar las actividades básicas de la vida diaria
Escala Barthel
Actividades que realiza
Baremo de movilidad reducida y dificultad para hacer uso del transporte público.
Productos de soporte
Otras necesidades derivadas de la discapacidad
Uso del Sistema Braille
Competencia en uso del Sistema Braille
Dificultades de orientación
Seguimiento de las clases
Seguimiento del contenido de las clases
Seguimiento de las prácticas
Realización de los exámenes
Utilización del ordenador
Acceso a la información
Ayudas técnicas
Recibe apoyo del servicio de atención a los alumnos con discapacidad
Recibe asesoramiento para su inserción laboral
Recibe alguna prestación económica
Recibe alguna becas
Recibe ayuda para el transporte
Recibe ayuda para financiar recursos técnicos

Nivel de seguridad medio
Recibe ayuda para financiar materiales docentes

Nivel de seguridad alto
Certificado de discapacidad
Otros documentos acreditativos
Tipo
Grado
Pronóstico de evolución
Medicación
Vinculación a la red pública o profesional de la salud mental
Estrategias de enfrentamiento al estrés
Otras necesidades derivadas de la discapacidad física
Recursos técnicos para acceder a la información oral
Cuáles
Lengua de signos
Competencia en lengua de signos
Lectura labial
Competencia en lectura labial
Sistema de comunicación principal
Dificultades al hablar
Dificultades de comprensión del habla
Dificultades de orientación
Otras necesidades derivadas de la discapacidad auditiva
Tipo de discapacidad visual
Otras necesidades derivadas de la discapacidad visual

Requisitos legales en la recogida de datos

Como punto de partida, se considera que las universidades públicas españolas ya realizan adecuadamente y de acuerdo con la normativa vigente, la recopilación de los datos de sus alumnos siguiendo los procesos y formularios

propios de cada una de ellas (formulario de matrícula, formularios de los servicios de atención, etc.). Todos estos datos ya disponibles en las respectivas instituciones y enumerados en el apartado anterior serán los que alimentaran el repositorio del sistema propuesto siendo lo más efectivo que las propias universidades sean las que los provean.

Para que todo este conocimiento tenga la fiabilidad y credibilidad necesarias debe ser veraz, completa y coherente. Es imprescindible dotar al sistema de suficiente inteligencia como para evitar duplicidades, pérdidas de información o bien ofrecer información contradictoria. Debido a ello el órgano gestor (OGR) debe tener acceso a toda la base de datos para revisar, contrastar y en caso de detectar anomalías volver a solicitar la información comprometida a la institución responsable.

Al mismo tiempo debe garantizar-se preservar la confidencialidad de los datos y por lo tanto no debe ser posible asociarlos a la persona física a la que corresponden.

Las dos premisas anteriores conllevan un problema ya que su aplicación nos plantea una contradicción. ¿Cómo puede el OGR gestionar la información contenida en el sistema manteniendo la disociación de los datos? Para solucionar este problema ha sido necesario desarrollar un Gestor de Agregación (GA). Este ente permite que durante el procedimiento de obtención de información desde las distintas universidades como con su ulterior consulta, ningún dato agregado pueda asociarse con ninguna persona en concreto. Por otro lado, del proceso de agregación ninguna universidad podrá obtener datos personales de alumnos matriculados en alguna otra.

Contar pues con el gestor de agregación permite al sistema la gestión, la cesión y comunicación flexible de la información, de forma agregada y anónima, a los actores interesados. Las universidades son Responsables de los Ficheros Primarios (con las medidas de seguridad prescritas según el RD 1720/2007 (Boletín Oficial del Estado, 2008)). El OGR deberá firmar un Contrato de Confidencialidad con cada una de las fuentes de información, reconociéndose como Encargado de tratamiento de los Ficheros.

Por otra parte cada universidad participante debe garantizar al OGR que los datos han sido recogidos y cedidos con el conocimiento y consentimiento de los alumnos.

Los contratos entre las partes deberán regular igualmente el compromiso para la actualización periódica pautada de los datos incorporados en el sistema.

Requisitos en los modelos documentales

Serán necesarios ciertos documentos que den cobertura legal al sistema. Por parte del Órgano Gestor del Repositorio será necesario contar con:

- Documento de seguridad (como los datos son disociados el nivel de seguridad a considerar es el básico).
- Alta del fichero del alumnado en la Agencia Española de Protección de Datos.
- Alta de fichero de usuarios del Sistema Información Global Universidad y Discapacidad (INUDIS) en la AEPD, con nivel de seguridad básico y automatizado).
- Disponibilidad del modelo de contrato reconociéndose como encargado de tratamiento (Anexo I).
- Disponibilidad de modelo de contrato con empresas / colaboradores de servicios externos (Anexo I).

Por otro lado las universidades participantes deberían disponer de:

- Documento de seguridad (el nivel de seguridad es alto en este caso ya que los datos no son disociados).
- Disponibilidad de modelo de recogida de datos de los estudiantes, con las leyendas indicando sus finalidades (incluidas en el Anexo I).

Disponibilidad de modelo de contrato con empresas / colaboradores de servicios externos.

DISEÑO DEL SISTEMA DE INFORMACIÓN

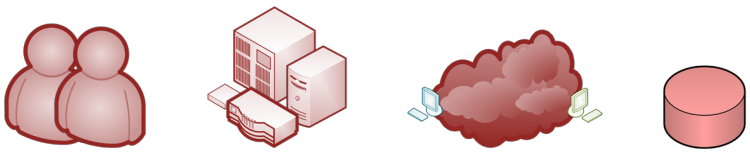
El diseño de un servicio de información estadística relativo al alumnado del sistema universitario español debe realizarse en base a dos premisas básicas: garantizar el cumplimiento de la normativa específica vigente y la eficiencia de la solución final. A nivel normativo, deben aplicarse exhaustivamente los requerimientos preceptivos en materia de seguridad debido a la naturaleza altamente sensible de los datos que gestionará el sistema de información. Mientras que a nivel de eficiencia debe priorizarse una solución que optimice la relación complejidad y coste de implementación versus las prestaciones reales a los usuarios del servicio.

A continuación se presentan las reflexiones sobre el escenario de trabajo, necesarias para justificar el diseño final; el diseño de la arquitectura del sistema; la formulación de los protocolos de seguridad; y la definición de la base de datos del sistema.

Escenario de trabajo

El escenario de trabajo contempla la interacción de cuatro categorías de elementos (Ilustración 1): los usuarios, los equipos, las comunicaciones y los datos. Los usuarios son el elemento clave, puesto que de ellos dependen, en última instancia, el uso del sistema. La infraestructura necesaria engloba a equipos y sistemas de comunicaciones. Mientras que los equipos estarán ubicados en las entidades que conformen el sistema de información, se considera que las comunicaciones estarán gestionadas por un operador externo, no teniéndose un control estricto de su configuración y uso. Finalmente, los datos, tanto académicos como de soporte de gestión, son los elementos que aportan valor al sistema.

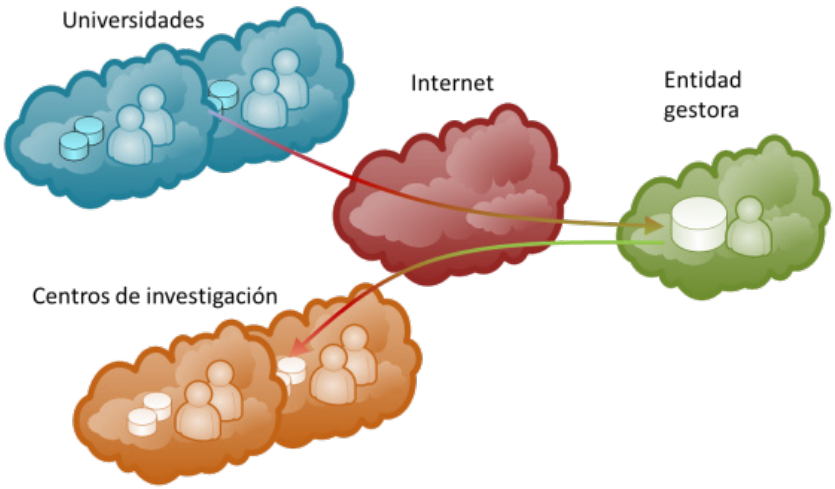
Ilustración 1. Elementos del sistema: usuarios, equipos, comunicaciones y datos.



El servicio de información se articula alrededor de tres grupos de usuarios: las universidades, centros de investigación y una entidad gestora. Las

universidades son la fuente de información del servicio. Cada una de ellas aporta los datos académicos de su alumnado y es responsable de la veracidad de dichos datos. Los investigadores reciben datos estadísticos agregados sobre el alumnado de las universidades, no contemplándose la posibilidad de aportar información al servicio. Los administradores, de la entidad gestora, gestionan los equipos y comunicaciones del servicio. A pesar de tener acceso a las bases de datos, no pueden identificar datos personales de estudiantes individuales, puesto que en las fases iniciales se han disociado los datos académicos de los datos personales. La entidad gestora debe pertenecer a la administración pública como requisito imprescindible. La Ilustración 2 esquematiza la relación entre estos usuarios. Nótese que se asume que la comunicación se realiza a través de un canal no seguro, Internet. Además, cada usuario se responsabiliza de la seguridad de sus sistemas, la integridad de sus datos y el buen uso de la información.

Ilustración 2. Esquema de relación entre usuarios.



Requisitos de seguridad

El servicio de información debe garantizar la seguridad de los datos que contiene. Para ello es necesario definir en qué consistirá dicha seguridad. En sentido amplio, la seguridad del servicio contempla desde la elección de los usuarios y el uso que ellos realizan del sistema; la adecuación normativa (eléctrica, mecánica, etc.); el mantenimiento -tanto hardware, como software o copias de respaldo- de los equipos; y la gestión de los datos. Es justamente en los aspectos directamente involucrados en la correcta gestión de los datos donde se profundiza a continuación.

En este sentido, las principales amenazas que debe contemplar el servicio de información son: el revelado o uso ilegítimo de la información; la violación de la integridad de los datos; la suplantación de la identidad de los usuarios y la denegación de servicio de los sistemas. Nótese que las amenazas se centran en qué se hace con la información y quien puede hacerlo.

Garantizar el secreto perfecto de la información almacenada es posible, aunque altamente costoso, como demostró C.E. Shannon en 1948. Para ello deben garantizarse cuatro premisas: la clave secreta para acceder a los datos solo se puede usar una vez; la clave es independiente del mensaje; la longitud de la clave es igual o mayor que el mensaje; y un posible atacante solo tiene acceso a la información cifrada. Por todo ello, los recursos necesarios para mantener operativo tal servicio de información están fuera del alcance de la gran mayoría de instituciones.

Por tanto, debe racionalizarse el nivel de seguridad a aplicar en el servicio de información. En una primera aproximación, pueden definirse cuatro niveles de seguridad: una seguridad incondicional, como la anteriormente expuesta, asumiendo un altísimo coste; una seguridad computacional, que fundamenta su valor en que el tiempo necesario para burlarla es muy superior a la vigencia de los datos, a un coste razonable; una seguridad probable, en que se presupone una moderada capacidad atacante; y una seguridad condicional, en que se acota la seguridad a un escenario restringido. Si se analizan los requerimientos legales, se concluye que el servicio de información debe disponer de un nivel de seguridad computacional.

Debe reflexionarse también sobre en qué elementos debe concentrarse la seguridad. El diseño del sistema establece dos niveles de seguridad: un nivel principal en los datos y uno secundario en su acceso remoto.

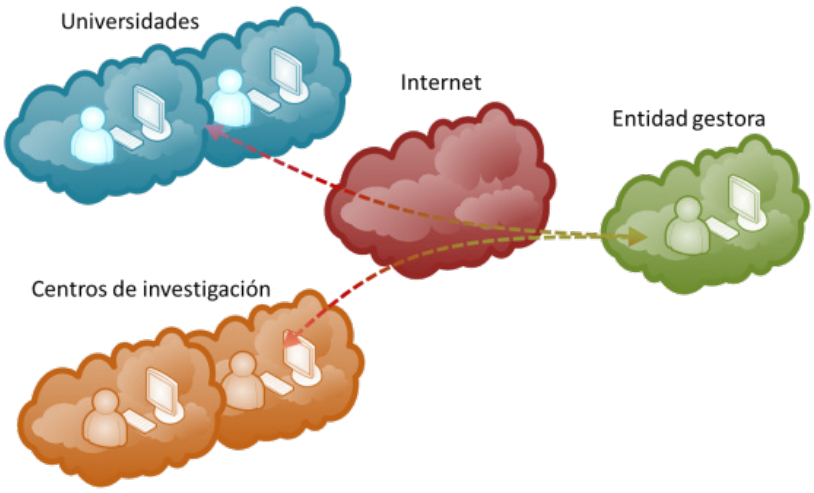
Para garantizar los requerimientos legales en las bases de datos se proponen dos mecanismos: la disociación de los datos personales/académicos y el cifrado de los datos. La disociación de los datos de los alumnos pretende separar la identidad de los alumnos de sus datos académicos. Mientras que las identidades de los alumnos deben almacenarse y gestionarse únicamente desde las universidades respectivas, los datos académicos a analizar pueden almacenarse también en las bases de datos de la entidad gestora a partir de identificadores unívocos. De esta forma los administradores de la entidad gestora solo tendrán acceso a datos académicos disociados. Los investigadores solo podrán acceder a datos académicos disociados y presentados de forma agregada. Si además estos datos se almacenan de forma cifrada, se garantiza una protección adecuada frente a posibles accesos no autorizados desde los equipos locales .

La seguridad en los sistemas de comunicación del servicio de información debe responder a dos tipos de ataques: los pasivos y los activos. Los ataques pasivos son aquellos en los que un usuario atacante centra se actividad en interceptar la información del servicio de información sin dejar rastro (solo "escuchando"). Son ataques difíciles de detectar y que tienen un éxito limitado, dependiendo del conocimiento del sistema implementado. En ataques activos los usuarios atacantes intentan confundir o interrumpir al sistema. Mediante la generación de información falsa o la modificación de información real los atacantes pretenden tanto introducirse en el sistema como alterar las bases de datos, pudiendo llegar a colapsar el servicio y provocar que éste no responda a peticiones de usuarios registrados.

De las reflexiones anteriores se plantean seis requisitos generales de seguridad: disponibilidad, se garantiza el acceso al servicio; autenticación, certifica la identidad de los usuarios; control de acceso, discrimina qué usuarios tienen acceso a ciertos recursos del sistema; no repudio, registro de actividad entre usuarios y el sistema; confidencialidad, los datos no son revelados a usuarios no autorizados; e integridad, se mantiene la consistencia de los datos.

Es necesaria una última reflexión en el planteamiento del servicio. La entidad gestora debe centralizar la seguridad del sistema (Ilustración 3), definiéndose como entidad certificadora local. Debe ser la responsable de la generación y distribución los certificados entre los usuarios. Así como de garantizar la consistencia e integridad de los datos del alumnado, pudiendo cotejar las aportaciones de cada universidad y evitar errores estadísticos. Nótese que generar el certificado no implica conocer el certificado. De hecho, su papel consiste en aportar las herramientas y garantizar su validez.

Ilustración 3. Distribución de claves.



Identificación unívoca del alumnado

Un primer problema a resolver consiste en obtener un sistema que permita identificar de forma unívoca a todos los estudiantes. Esta problemática surge debido a la diversidad de procedencias y situaciones del alumnado. En principio todo alumno (sea comunitario o no) matriculado en una Universidad española ha de poseer al menos uno de los siguientes documentos:

1. Documento Nacional de Identidad (DNI)
2. Tarjeta de Identidad de Extranjero (TIE/NIE)[3]
3. Pasaporte
4. Documento de identidad de su país de origen

De ello se desprende que un código adecuado para identificar de forma única a un alumno (*IUA*) sería concatenar a la fecha de nacimiento el primero de los documentos citados disponible (según el orden anterior), eliminando cualquier carácter NO numérico del mismo. Es decir, sólo pueden aparecer los caracteres ASCII compendios entre 48 y 57. La fecha se codificará también únicamente con caracteres numéricos según el formato *ddmmaaaa*.

3 El NIE (Número de Identidad de Extranjero) es el número que aparece en el TIE. Puede ocurrir que no se disponga de TIE pero sí de NIE, por eso en la codificación se usa el NIE.

Para evitar que dos alumnos que tengan el mismo número de documento (sin letras) y hallan nacido en la misma fecha se confundan, antes de codificar el documento de identidad se antepondrá un 1 si es un DNI, un 2 si es un NIE, un 3 si es un pasaporte y un 4 si es otro documento.

Por ejemplo:

- A un alumno nacido el 12 de agosto de 1990 con DNI 99999990-S le correspondería el *IUA*=12081990199999990
- A un alumno nacido el 3 de julio de 1994 con NIE X-9999990-G (y sin DNI) le correspondería el *IUA*=0307199429999990

Proceso de agregación anónima de los datos

El almacenamiento de datos personales está regulado por la *Ley Orgánica de Protección de Datos de Carácter Personal* de 1999, según se indica en el correspondiente apartado del presente documento. En esta descripción se da por sentado que cada Universidad almacena los datos de sus alumnos cumpliendo la normativa vigente y, por tanto, el sistema de agregación de los mismos debe diseñarse para que ningún dato personal almacenado por una Universidad pueda ser identificado fuera de su ámbito. Para ello es imprescindible que, tanto durante el procedimiento de obtención de información desde las distintas universidades como con su ulterior consulta, ningún dato agregado pueda asociarse con ninguna persona en concreto. Por otro lado, del proceso de agregación ninguna universidad podrá obtener datos personales de alumnos matriculados en alguna otra. La entidad que permitirá la agregación anónima (disociación de datos personales y posterior agregación de datos académicos) será la Entidad Gestora.

El objetivo de la agregación anónima es que durante el proceso y ulterior consulta se satisfagan las siguientes condiciones:

1. La Entidad Gestora (encargada de la recopilación de los datos de las distintas universidades) no ha de poder asociar dichos datos con ninguna persona en concreto.
2. Ninguna Universidad ha de ser capaz de asociar datos de otra aunque provengan de la misma persona. Es decir, ni el proceso de agregación ni una posterior consulta a los datos puede aumentar la información que de un alumno tenga una Universidad.

3. La Entidad Gestora ha de poder unificar los datos de las distintas Universidades que pertenezcan a la misma persona, pero ha de ser incapaz de asociarlos a alguien en concreto.

Las partes integrantes del sistema en este punto son:

- Entidad Gestora: *EG*
- Conjunto de Universidades: U_i, $i=1....n$

En una fase previa, cada universidad genera de forma autónoma y secreta su par de claves pública y privada. Cuando una Universidad se asocia al sistema de información, la *EG* debe proporcionarle un certificado digital X.509 generado a partir de la clave pública que dicha universidad le ha proporcionado. Este certificado se almacena en el Repositorio de Acceso Restringido para estar disponible al resto de integrantes del sistema. Nótese que *EG* genera el certificado, pero desconoce las claves privadas de las universidades. El procedimiento para la generación de los mismos se detalla en el Anexo II. Además, se mantiene la premisa que las Universidades cooperan honestamente y que ninguna de ellas pretende sabotear el sistema[4].

Desde un punto de vista funcional, la comunicación previa a la agregación anónima entre los miembros del sistema de información puede llevarse a cabo mediante múltiples implementaciones. En cualquier caso, debe realizarse mediante un repositorio de acceso restringido (*RAR*) a las partes implicadas (*EG* y U_i's). Estrictamente sólo es necesario que la escritura esté controlada ya que el diseño del protocolo hace la lectura del mismo sea irrelevante para la seguridad. Inicialmente en el RAR se almacenaran las claves públicas y certificados de todas las entidades del sistema de información.

Una vez que todas las Universidades comparten sus certificados digitales certificados por la EG, el siguiente paso consiste en la obtención de un secreto compartido entre todas las Universidades y que resulte desconocido para la Entidad Gestora[5].

---

4 Aunque el diseño del protocolo garantiza que ninguna universidad pueda obtener datos de otra de forma fraudulenta no protege frente, por ejemplo, a la inclusión de datos falsos o erróneos.

5 Si una Universidad revela el secreto a la EG ésta podrá asociar los datos personales con un esfuerzo limitado (e.g.. probando con todas las fechas y números de documento posibles)

Para ello la Entidad Gestora selecciona una universidad al azar y le delega la generación de un Prefijo Secreto (PS). Para generar el prefijo secreto se propone usar la función SHA-1 de un número aleatorio. El resultado será un número de 160 bits que se expresará en 40 cifras hexadecimales precedidas por los ceros necesarios.

Un vez dicha universidad ha calculado PS, lo distribuye entre el resto de Universidades depositando un mensaje para cada universidad en el RAR. Los mensajes los genera firmando el Prefijo Secreto y cifrando el conjunto con la clave pública de cada universidad, obtenida del certificado compartido correspondiente. Nótese que en este punto, en el RAR se almacenan los certificados de Universidades y EG, así como los PS cifrados de las universidades. De este modo, cada universidad puede obtener PS descifrando el mensaje que va dirigido a ella y verificar que PS lo ha generado la Universidad delegada a tal efecto. Además, se garantiza que EG desconoce PS.

Una vez que todas las Universidades conocen PS proceden de la siguiente forma para poder disociar los datos de la información personal: cada Uj (j=1...n) obtiene un certificado X.509 de la EG según se explica en el Anexo 1

Una vez que todas las Universidades conocen *PS* proceden de la siguiente forma para poder disociar los datos de la información personal:

1. Cada *Universidad* calcula el Identificador Único de Alumno (*IUA*) según lo expuesto anteriormente.

2. Cada *Universidad* antepone *PS* al *IUA* para calcular el Identificador Pseudoaleatorio ID_{ps} como el hash: ID_{ps}=SHA-1(*PS*||*IUA*). El resultado también se expresará en 40 cifras hexadecimales precedidas por los ceros necesarios. Nótese que de esta forma la *EG* no puede recuperar el *IUA* a partir del ID_{ps} (ni siquiera probando con todas las fechas y números de documento posibles) y, por tanto, los datos personales quedan disociados de cualquier persona física para todo aquél que desconozca *PS* (las Universidades deben mantenerlo en secreto).

3. Una vez sustituidos los *IUA* (y, obviamente, cualquier otro identificador personal como el nombre) por los ID_{ps} los datos quedan disociados de la identidad física por lo que ya no se trata de datos personales.

4. Cada Universidad transmitirá sus datos a la EG cifrados con la clave pública de EG disponible en el RAR para evitar que terceros pudieran correlacionar datos académicos. Puede utilizarse, por lo tanto, el RAR

como repositorio temporal de los datos antes de cargarlos en la base de datos principal.

5. Para evitar que alguna Universidad pueda identificar datos almacenados en otra a partir de los datos agregados en la base de datos, la *EG* no almacenará los ID_{ps} (pues son conocidos por todas las U_i's) sino su Identificador Agregado Anónimo ID_{agran}=AES256_K_{EG}(ID_{ps}) usando una clave secreta K_{EG} elegida por ella misma. El resultado de ID_{agran} es un número binario de 128 bits que se expresara en 32 cifras hexadecimales precedidas por los ceros necesarios.

Equipos y comunicaciones

La seguridad en equipos y comunicaciones dependerá de varios factores: de la elección de los equipos, de la topología de red en que se interconecten y de los protocolos de comunicación que utilicen. Del análisis preliminar de la Ilustración 2 y la Ilustración 3 puede observarse que existen tres entornos diferenciados: el entorno de cada universidad, el entorno del operador de telecomunicaciones y el entorno de la entidad gestora. El análisis que se describe a continuación solo detalla el entorno de la Entidad Gestora, ya que es del único del que puede responsabilizarse.

Debido a que la Entidad Gestora utiliza Internet como canal de comunicaciones, y es inherentemente inseguro, todas las comunicaciones entre los miembros del sistema de información se deberán realizar mediante protocolos que incorporen SSL/TLS con certificados X.509 en ambos extremos (ssh, https, sftp, openvpn, etc). De esta forma, quedarán garantizadas tanto la autenticación mutua de los comunicantes como la privacidad e integridad de los datos transmitidos.

Se ha escogido una topología de red Screening Subnet Firewall, tal como muestra la Ilustración 4. Se propone implementar esta topología con siete equipos: dos cortafuegos, cuatro servidores y una cabina de discos. Esta topología divide la red interna de la Entidad Gestora en dos segmentos: uno interior seguro y uno exterior susceptible de ser atacado.

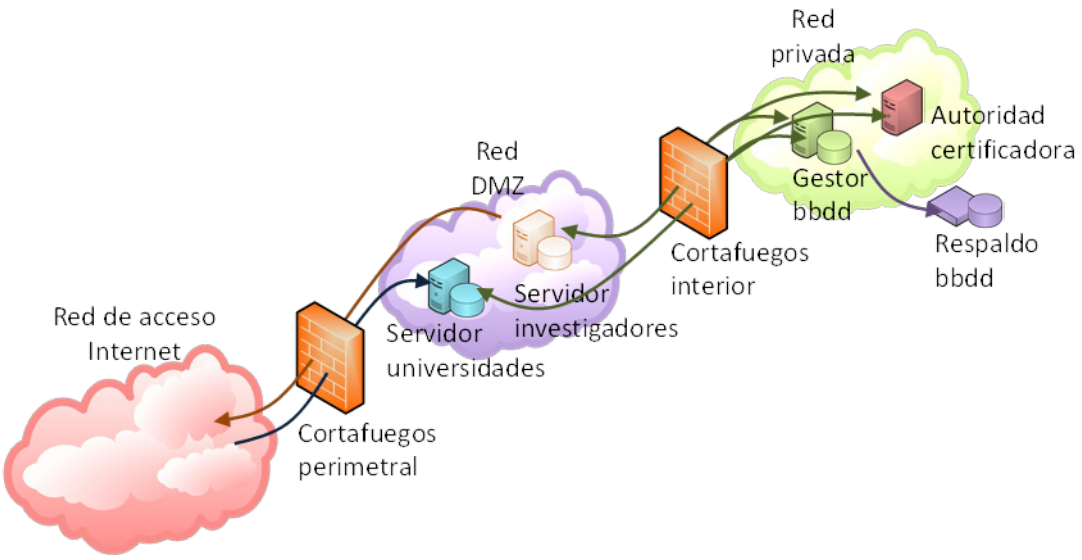
El segmento exterior, denominado Zona DesMilitarizada (DMZ), es parcialmente accesible desde la red de acceso (Internet). Es en la DMZ donde se encuentran los servidores a los que accederán las universidades y los centros de investigación. Los equipos que se ubiquen en la DMZ son denominados Bastion Hosts, ya que se considera que deben protegerse de forma exhaustiva, pues es muy probable que sean atacados. Los cortafuegos impedirán que una comunicación procedente de la red de acceso consiga

llegar al segmento interior, la red privada. Solo las comunicaciones originadas en los Bastion Hosts podrán penetrar en el segmento interior.

El segmento interior, la red privada, es donde se ubican los servidores principales de la Entidad Gestora. En ella se encuentra la base de datos académicos y la Autoridad Certificadora del sistema de información. Estos servidores teóricamente están fuera de peligro y pueden centrar sus recursos en la gestión del servicio.

Los cortafuegos controlan muy estrictamente las comunicaciones entrantes (Internet→DMZ y DMZ→privada) respectivamente. Aunque puede relajarse la seguridad respecto las comunicaciones salientes (privada→DMZ y DMZ→Internet) para agilizar procesos de actualización, consultas externas, etc.

Ilustración 4. Topología la red de la Entidad Gestora



Analizando el esquema, el equipo más expuesto a posibles ataques desde Internet es el cortafuegos perimetral. Este equipo es el responsable de proteger a la Entidad Gestora frente a posibles ataques desde Internet. Solo permite comunicaciones mediante protocolos específicos desde Internet hacia puertos concretos de los servidores de universidades e investigadores.

Seguidamente se disponen los Bastion Hosts. Estos dos servidores son la puerta de acceso a universidades y centros de investigación. Se han estructurado en dos equipos para separar físicamente ambos grupos de usuarios. Contienen las interfaces del sistema con las que interactuarán los usuarios. El servidor de universidades contiene, además, el Repositorio de Acceso Restringido, necesario para la agregación anónima. Estos servidores se comunicarán con los servidores principales (el gestor de la base de datos y la

Autoridad Certificadora) para realizar las operaciones solicitadas por los usuarios, aislando a los servidores principales del acceso directo de los usuarios.

El cortafuegos interior protege a los servidores principales ubicados en la red privada, de posibles intrusos que hayan podido atravesar el firewall perimetral. Es recomendable que sea un modelo diferente que el cortafuegos perimetral para maximizar las capacidades defensivas del sistema.

En la red privada se encuentran tres equipos: el Gestor de la base de datos, la Autoridad Certificadora y una cabina de discos. El Gestor de la base de datos administra y almacena la base de datos académicos. Contiene datos agregados anónimamente, tal como se ha descrito en la sección anterior. La Autoridad Certificadora es el núcleo de la seguridad de los datos de la Entidad Gestora. Los usuarios del sistema de información reconocen a este equipo como referente local para cifrar y firmar los datos. Nótese que los certificados usados se basan en esta relación de confianza, y por consiguiente toda la seguridad en la agregación anónima. La cabina de discos es la responsable de mantener copias de seguridad de la base de datos académicos y de los certificados.

Evidentemente, toda esta infraestructura depende, en última instancia, de los administradores del sistema. A los cuales se les debe otorgar la confianza necesaria para poder ejercer su función.

Requerimientos de diseño del modelo de datos

La definición del modelo de datos es crucial a la hora de dotar de funcionalidad al presente sistema de información. Para definir dicho modelo con garantías y permitir un sistema estable y escalable, es imprescindible definir de forma clara y concisa cuales son las limitaciones del sistema y qué se espera de él. En esta sección se cubren estos aspectos desde los distintos ámbitos en los que se puede llevar a cabo dicho estudio.

Resumen de las principales reglas de negocio

Las reglas de negocio establecen el propósito de un sistema de información. A continuación se recogen las principales reglas de negocio relacionadas con el sistema propuesto.

- Se requiere de un conjunto exhaustivo de datos por alumno para que el sistema sea funcional. Los datos requeridos por alumno han

sido presentados en el apartado que hace referencia a los *requerimientos académicos* y serán ampliados cuando se presente el modelo de datos.

- Los alumnos podrán estar cursando diversos estudios de forma simultánea. No existe limitación en cuanto al número de estudios simultáneos por alumno.
- Cada alumno entregará los datos solicitados al *centro* en el que esté cursando sus estudios.
- Cada alumno proporcionará una copia de los datos indicados en el apartado de *requerimientos académicos*, para cada uno de los estudios que realice.
- Los investigadores tendrán acceso a todos los datos relevantes, si bien no podrán relacionar dichos datos con alumnos concretos.
- La entidad gestora podrá limitar, si lo considera oportuno, el acceso a ciertos datos que considere inapropiados para un determinado investigador.
- Los procesos de introducción de los datos por parte de los alumnos, de verificación de los mismos por los responsables de la entrada de datos en el centro en el que dichos alumnos cursan sus estudios, así como de su posterior carga en el repositorio de datos estarán acotados temporalmente de acuerdo a una planificación establecida por la entidad gestora del sistema.
- La planificación de todos los procedimientos deberá establecerse con una anterioridad de 3 meses antes de iniciarse éstos.
- Los datos identificativos de los alumnos estarán disociados con aquellos que son consultables en el repositorio.
- Sólo un conjunto de usuarios por centro, habilitados a tal efecto, tendrán acceso a los datos identificativos de los alumnos.
- Sólo un usuario por centro podrá firmar los datos, dando validez a los mismos.
- No se podrá conocer la identidad de un alumno a partir de los datos recogidos en el repositorio.
- Se conocerá el centro al que pertenecen los datos de alumno para notificar posibles inconsistencias de los mismos.

- Se tendrá que identificar unívocamente a un alumno para detectar múltiples cargas de datos relacionados con un mismo alumno. Del conocimiento de identificación no se podrá derivar la identidad del alumno.
- Los alumnos no podrán consultar sus propios datos a través del sistema, una vez remitidos éstos al centro en el que está cursando sus estudios. El centro deberá habilitar mecanismos alternativos para permitir esta funcionalidad.

Suposiciones

Existen un conjunto de circunstancias que se asumen como ciertas a la hora de diseñar el presente sistema de información. Pese a no ser requeridas de forma explícita, este conjunto de limitaciones debe indicarse de forma expresa con el objetivo de dotar de coherencia al modelo de datos presentado más tarde. Las principales suposiciones establecidas en el presente sistema de información se detallan a continuación:

- El sistema operará con interfaces basadas en un ecosistema web. Dichas interfaces cumplirán con las recomendaciones recogidas en la norma ISO/IEC 40500 (equivalente a las recomendaciones *Web Content Accessibility Guidelines (WCAG)* en su versión 2.0). En concreto se deberá satisfacer un nivel de conformidad AAA conforme a dicha normativa.
- Los distintos usuarios del sistema cuentan con acceso a Internet y, además, poseen los conocimientos básicos de navegación por la web.
- Para registrarse en el sistema, los usuarios conocen y aceptan los términos establecidos por el mismo, por lo que tienen conocimiento de las obligaciones y derechos que implica ser parte un usuario registrado.
- La entidad gestora del sistema tiene la potestad de iniciar las acciones que consideren oportunas contra aquellos usuarios que incumplan las normas establecidas para el uso del sistema.
- Los usuarios del sistema introducen información veraz.
- El sistema no puede garantizar la veracidad de los datos contenidos, si bien realizará tantas acciones como sea necesario para detectar posibles inconsistencias en los datos aportados.

- El sistema proporcionará mecanismos con los que corregir anomalías en los datos almacenados.

Requerimientos no funcionales

Este apartado recoge los distintos requerimientos no funcionales relacionados con el diseño del sistema. Dichos requerimientos vienen a completar a los ya presentados anteriormente, relacionados con la actividad académica, los aspectos legales y los relacionados con la seguridad del sistema.

Requerimientos de experiencia de usuario

El sistema a desarrollar será utilizado por un conjunto heterogéneo de usuarios, tanto por su nivel de formación, como por sus capacidades. De esta forma, el sistema deberá satisfacer los siguientes requerimientos, cuyo detalle específico puede consultarse en el Anexo II.

Uniformidad de la interfaz

Un aspecto uniforme de la interfaz facilita la navegación al usuario y proporciona una imagen de consistencia que mejora la experiencia del software. De esta forma, la interfaz a desarrollar deberá seguir un mismo patrón de diseño para todas sus vistas, de manera que no haya ninguna que desentone del resto. Esto también incluye la paleta de colores y el posicionamiento de los bloques que componen cada vista.

Paleta de colores agradable

Los colores pueden tener un impacto enorme en la opinión de la gente y en su estado de ánimo. Las paletas de colores juegan un papel importante porque si la combinación de colores no es suficientemente agradable, habrá un fuerte rechazo por parte de los usuarios. De esta forma, la paleta de colores deberá tener matices claros y agradables, así como el contraste apropiado. De igual forma, los matices de dicha paleta deberán poder ser apreciados por todo tipo de usuarios, con independencia de sus capacidades visuales en cuanto a captación del color.

Claridad en la información textual

Si la interfaz del sistema tiene contenido escrito con fuentes demasiado pequeñas, o de tipos poco frecuentes, o con colores demasiado llamativos, los usuarios tendrán dificultades para leer el contenido mostrado,

generándose así una resistencia al uso del sistema. De esta forma, todos los textos mostrados a través de las interfaces del sistema deberán ser fácilmente legibles, empleando para ello una tipografía clara y conocida que permita evitar forzar la vista a los usuarios que emplean el sistema.

Interfaz amigable e intuitiva

Es imprescindible que la interfaz se muestre consistente, sencilla y eficaz con respecto a la operativa que de ella hace el usuario.

Visibilidad del estado del usuario

La mayor parte de la funcionalidad requiere de un usuario identificado. Por lo tanto, esta acción debe ser lo más simple posible. De esta forma, el estado del usuario deberá estar claramente visible. Si está identificado, ésta condición debe ser claramente visible. En caso contrario, se indicará claramente cómo autenticarse en el sistema para así iniciar una sesión. La opción de finalización de la sesión (cerrar la sesión o *logout*), así como las opciones asociadas con la información del usuario también estarán siempre visibles una vez éste se acredite.

Ayuda siempre presente

Existe una alta heterogeneidad de usuarios y se esperan grandes diferencias en sus conocimientos. Por lo tanto es imprescindible clarificar en la medida de lo posible las acciones tomadas. De esta forma, el usuario deberá poder obtener información sobre el significado de las acciones que se espera de él así como un área de ayuda general. Esta serie de ayudas deberán estar disponibles en todas las secciones de cualquiera de las interfaces empleadas.

Procedimientos definidos

Desconocer el conjunto de pasos realizados o pendientes en una operación puede desmotivar y desorientar al usuario, lo que redunda en una experiencia negativa de uso. Por lo tanto, el usuario debe tener claro todos los pasos a seguir para alcanzar un determinado propósito. De esta forma, la interfaz deberá mostrar tanto los pasos realizados como los que quedan por realizar, de tal forma que el usuario conozca en todo momento el camino a seguir y se sienta cómodo empleando la interfaz.

Resumen y confirmación por acción

Presentar un resumen de la acción permite de forma rápida que el usuario verifique los pasos realizados y se asegure de que éstos sean correctos. La confirmación establece un mecanismo de verificación que obliga al usuario a atender a los datos introducidos. Por lo tanto, al finalizar toda acción, el sistema presentará un resumen de la acción y solicitará una confirmación al usuario. Con ello se pretende asegurar la integridad de las acciones llevadas a cabo y de los datos almacenados en el repositorio.

Selección de idioma

Adecuar el idioma de la aplicación a las necesidades o costumbres del usuario mejora notablemente la experiencia de usuario. Por lo tanto, la aplicación deberá estar disponible en, al menos los siguientes idiomas: catalán, gallego, vasco, español e inglés.

Sencillez de la interfaz

La sencillez de la interfaz redunda en un menor número de incidencias, así como en una mejor experiencia de usuario, maximizando el rendimiento que éste extrae del sistema. Por lo tanto, el sistema tendrá una interfaz sencilla y comprensible para cualquier tipo de usuario.

Límite en el número de páginas

Los procedimientos funcionales deben estar limitados en cuanto al número de páginas de información mostrada o solicitada al usuario. Procedimientos demasiado extensos merman la concentración y el interés de los usuarios. De esta forma, no habrá ningún caso de uso en el sistema que requiera de un número de páginas superior a 5 para su correcta finalización.

Requerimientos de rendimiento

Tiempo de respuesta reducido

Grandes latencias en un sistema como el descrito provocan que el usuario reduzca su productividad y aumente la desidia con respecto al uso del sistema, que ven más como un impedimento que como una solución. Por consiguiente, el tiempo de respuesta del sistema debe de ser lo suficientemente rápido como para seguir el nivel de actividad del usuario. Se establecerá por tanto un límite en el tiempo de respuesta, de forma que su

valor medio sea de 0,50 segundos y bajo la premisa de que dicho tiempo no podrá exceder los 5 segundos bajo ningún concepto.

Subsistemas separados

Cada subsistema gestiona un tipo de información distinto en cuanto a sensibilidad y por tanto está sujeto a exigencias distintas en cuanto a seguridad. Además, se espera que el subsistema *entrada de datos* sea local, lo que redunda aún más en la justificación de la separación del hardware que ha de darle soporte. De esta forma, cada uno de los dos subsistemas, el de *repositorio de datos* y el de *entrada de datos*, dispondrá de un servidor específico.

Requerimientos operacionales y de entorno

Compatibilidad con los principales navegadores

Cada usuario empleará de forma instintiva su navegador habitual para operar. La experiencia de usuario podría empeorar en caso de que éste no funcione correctamente, hasta llegar al punto de no emplear el sistema, siendo esto crítico en el caso del usuario alumno, encargado de facilitar la base de los datos que posteriormente que se almacenarán en el repositorio. De esta forma, la interfaz del sistema se basará en una aplicación web, que deberá visualizarse y operar correctamente en los cuatro navegadores más populares del mercado: Chrome, Microsoft Explorer, Firefox y Safari.

Instalación del subsistema entrada de datos

La parte del sistema (subsistema) referente a la entrada de datos define una serie de operaciones relacionadas con la gestión del a información proporcionada por los alumnos. Por lo tanto debe estar desplegado antes de que éstos proporcionen dicha información. En caso de no estarlo, el sistema deberá proveer de un mecanismo adecuado para la importación de datos ya almacenados de forma local por las distintas instituciones usuarias del sistema.

Independencia del sistema de entrada de datos

La aplicación sólo da acceso al repositorio. El subsistema *entrada de datos* sólo permite el acceso a los usuarios *entrada de datos* y *alumno* vinculados al centro educativo en el que se encuentra desplegado. Con el objetivo de mejorar la seguridad y la operatividad del sistema, los distintos sistemas de entrada de datos no serán visibles entre ellos.

Datos del alumno no consultables por éste

Los alumnos proporcionan información al sistema, siendo por tanto la base de funcionamiento del mismo. Sin embargo, su actuación se reduce a la mera provisión de datos, no esperándose de ellos ninguna operación adicional. De esta forma, los datos del alumno no serán consultables por éste una vez los haya remitido al subsistema entrada de datos.

Especificación de la base de datos académicos

Usuarios

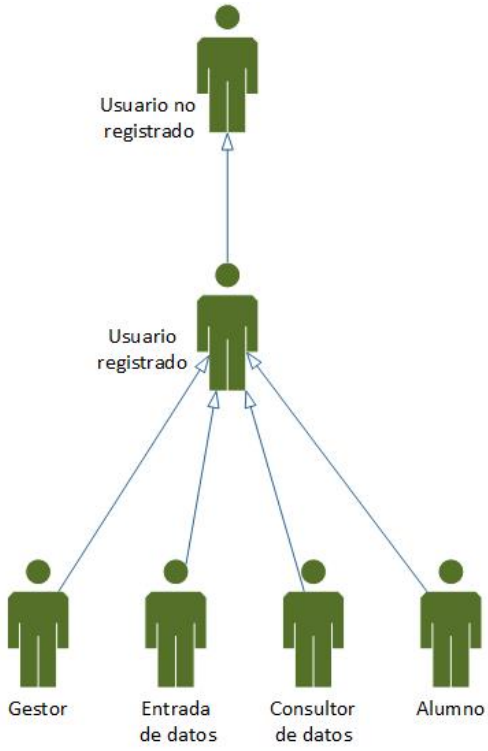
El sistema a definir contempla 4 actores claramente diferenciados de acuerdo a su rol:

- Gestor. Se considera usuario gestor al representante de la entidad gestora.
- Entrada de datos. Se corresponde con un usuario perteneciente a un centro enmarcado en una institución o universidad. Será el encargado de proveer al sistema de información con los datos recogidos en el centro/universidad al que dicho usuario pertenece.
- Consultor de datos. Este actor hace referencia a un investigador que consulta los datos guardados en el sistema de información. Este tipo de actor sólo podrá llevar a cabo acciones de consulta sobre el sistema, nunca de modificación de los datos allí almacenados.
- Alumno. Este actor se corresponde con un alumno que cursa estudios en un centro de una institución/universidad contemplada en el sistema de información. Este actor será el que proveerá de información individual a los distintos usuarios *entrada de datos*.

El sistema define un tipo de usuario por rol detectado. Además, cada usuario puede estar en dos estados claramente diferenciados: usuario registrado y no registrado. Un usuario no registrado es un usuario del mismo que carece de credenciales para el uso del sistema en operaciones privilegiadas (ej. introducción de datos, consulta de la información contenida en el sistema, etc.). Por el contrario, se entiende al usuario registrado como aquel que dispone de credenciales en el sistema, siendo éste capaz de identificarlo y darle acceso al conjunto de acciones que puede efectuar según su rol primario

(es decir, según sea alumno, consultor de datos, entrada de datos o gestor). De esta forma, el sistema de información contempla 6 tipos de usuario, cuya jerarquía final queda reflejada en la Ilustración 5

Ilustración 5. Jerarquía de usuarios.



Subsistemas

El sistema de información a definir se ha estructurado en dos subsistemas, cuyo objetivo es simplificar la especificación y posterior diseño de la solución software y su consiguiente modelo de datos. La división propuesta se ajusta a la planteada a la hora de diseñar la topología de la red que da soporte al sistema de información. Dichos subsistemas son:

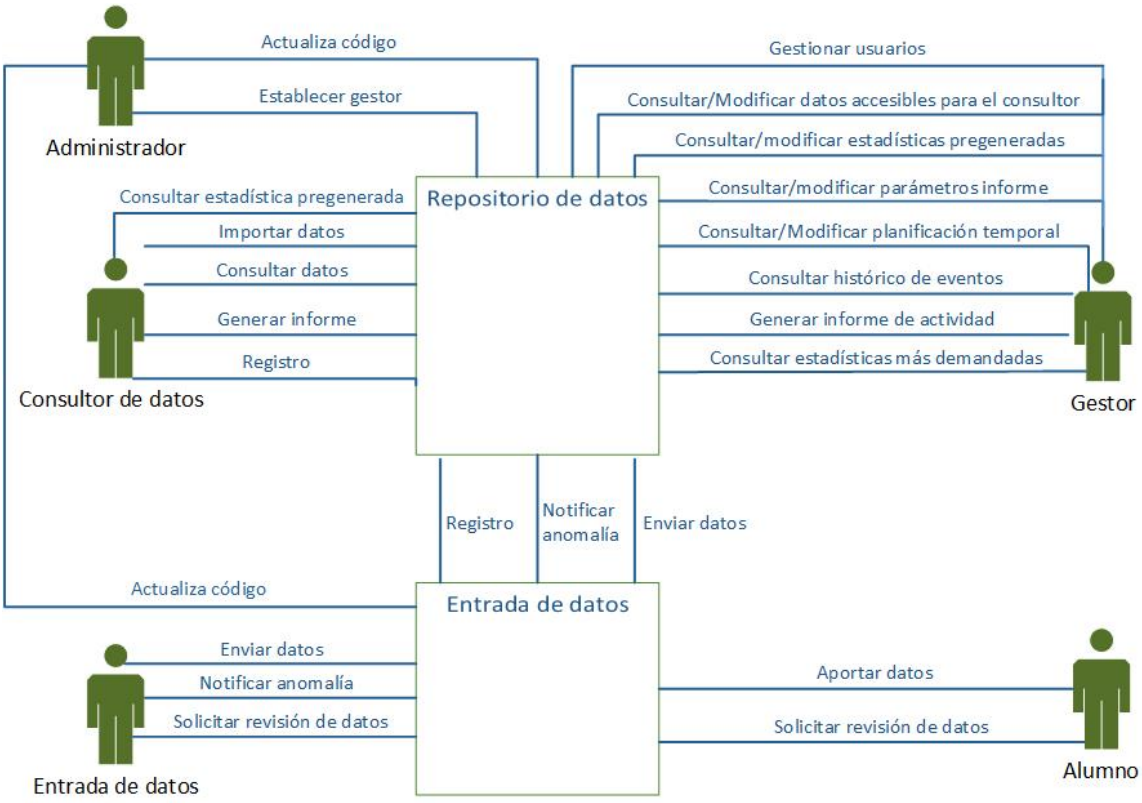
- Subsistema *entrada de datos*. Este subsistema engloba todas aquellas funcionalidades relacionadas con la introducción de los datos que se van a almacenar en el sistema, desde su captación hasta su transmisión y posterior almacenado en el repositorio de datos propiedad de la entidad gestora.
- Subsistema *repositorio de datos*. Este subsistema engloba todas aquellas funcionalidades asociadas directamente con el modelo de datos, es decir, aquellas acciones que implican la consulta o

modificación de los datos contenidos en el repositorio de datos propiedad de la entidad gestora.

Casos de uso principales

El sistema de información descrito abarca un gran número de funcionalidades, habida cuenta que alcanza tanto al sistema de almacenamiento de los datos, como a las entidades aprovisionadoras de los mismos y del alumnado del que finalmente se obtendrá la información, sin descuidar a los usuarios que harán uso de la información contenida, a través de procesos de consulta. La Ilustración 6 muestra de forma global en conjunto de funcionalidades ofrecidas por cada subsistema, así como los usuarios principales involucrados en las mismas.

Ilustración 6. Diagrama general de funcionalidad del sistema.



A continuación se describen las funcionalidades (casos de uso) más relevantes relacionadas con la operativa del sistema de información. Para una completa especificación de estos casos de uso, así como de otros casos de uso de menor relevancia no descritos en este documento, puede consultarse el Anexo II.

Registrarse

Esta funcionalidad permite a un usuario no registrado, registrarse con el objetivo de pasar a ejercer el rol de un usuario privilegiado del sistema. Este caso de uso sólo aplica al subsistema *repositorio de datos*. En el caso del subsistema *entrada de datos*, el caso de uso *registrarse* se considera propio de cada centro educativo donde se implante el software y por lo tanto su definición queda fuera del ámbito de este proyecto.

Login / Logout

Esta funcionalidad permite a un usuario registrado acceder al sistema, iniciando una sesión (*login*), o bien finalizar la sesión activa (*logout*). Cada uno de los subsistemas tendrá su propio caso de uso *login*. Lo mismo ocurrirá con el caso de uso *logout*. La verificación de las credenciales se realizará de forma independiente entre subsistemas. En el caso del subsistema *entrada de datos*, se asume que cada dispondrá de su propio mecanismo para cotejar las credenciales de sus usuarios. Las sesiones en cada uno de los subsistemas se considerarán independientes.

Importar datos

Mediante esta funcionalidad, el sistema transforma los datos recogidos por el subsistema *entrada de datos* en un formato compatible para su posterior carga en el subsistema *repositorio de datos*.

Firmar datos

Cualquier dato que quiera ser cargado en el repositorio de datos requiere de su firma previa. Esta firma tiene como objetivo garantizar el origen y la integridad de la información cargada. Dicha firma será realizada por un usuario del subsistema *entrada de datos* habilitado a tal efecto, mediante los mecanismos criptográficos descritos anteriormente.

Enviar datos firmados

Esta funcionalidad permite la carga de datos procedentes del subsistema *entrada de datos* en el subsistema *repositorio de datos*. Para ello, los datos tendrán que haber sido previamente firmados.

Notificar anomalía

Mediante esta funcionalidad, el subsistema *repositorio de datos* informa al subsistema *entrada de datos* de la detección de una anomalía en los datos proporcionados durante el último *envío de datos firmados*.

Gestionar estadísticas pre-generadas

Conjunto de funcionalidades mediante las cuales el *gestor* se encarga de definir un conjunto de consultas cuyo resultado (estadística) se generará sin que se produzca una petición expresa procedente de un usuario *consultor de datos*. El objetivo de estas acciones será mejorar la eficiencia del sistema, así como su experiencia de uso, proporcionando una serie de consultas de especial interés a los consultores de tal forma que dispongan de esa información de forma rápida y sencilla. Los criterios elegidos para definir estas estadísticas quedarán a merced de la entidad gestora, si bien se espera que residan en parámetros como la frecuencia de la demanda de los datos, el marco normativo vigente, etc.

Consulta estadística pre-generada

Mediante esta funcionalidad, un usuario consultor de datos puede acceder a un conjunto de estadísticas (es decir, consultas sobre el repositorio de datos) previamente generadas. De esta forma, el consultor puede obtener un conjunto de datos de forma rápida, sin necesidad de un conocimiento completo sobre el funcionamiento del sistema.

Consulta simple de datos

Mediante esta funcionalidad, el usuario puede obtener una estadística que dependa de dos variables cuya información esté incluida en el repositorio de datos (ej. evolución del número de alumnos con discapacidad visual en los últimos 10 años). El conjunto de datos disponibles para su consulta quedará determinado por la entidad gestora del sistema, si bien en un principio se asume la total disponibilidad de la información almacenada en el repositorio de datos.

Consulta compleja de datos

Mediante esta funcionalidad, el usuario *consultor de datos* puede obtener una estadística que dependa de más de dos variables cuya información esté incluida en el repositorio de datos (ej. evolución del número de alumnos con discapacidad visual en los últimos 10 años, agrupados por área de estudios). El

conjunto de datos disponibles para su consulta quedará determinado por la entidad gestora del sistema, si bien en un principio se asume la total disponibilidad de la información almacenada en el repositorio de datos. Esta funcionalidad exigirá un conocimiento amplio del funcionamiento del sistema, en tanto en cuenta que el *consultor de datos* deberá componer la consulta en tiempo real mediante las facilidades proporcionadas por el sistema.

Generar informe

Esta funcionalidad permitirá a un *consultor de datos* generar un informe con los datos que sean de su interés. Dichos informes, contendrán las estadísticas solicitadas por el usuario (pre-generadas, simples y/o complejas) y las explicaciones que de ella se deriven (en caso de ser requerido). Los informes generados estarán firmados por la entidad gestora del sistema, de forma que se pueda acreditar su autenticidad, y no serán manipulables.

Gestionar planificación temporal

El subsistema *repositorio de datos* incluye una serie de funcionalidades que tienen por objetivo definir la planificación temporal del sistema, de acuerdo a los requerimientos recogidos en apartados anteriores. De esta forma, la entidad gestora podrá consultar, establecer, modificar, borrar los límites temporales asociados con cada una de las fases operativas del sistema: carga de datos en el repositorio y consulta de los datos almacenados en el repositorio.

Así pues, un usuario *entrada de datos* sólo podrá enviar datos dentro del límite temporal asociado con la carga de datos. Durante ese periodo, el subsistema *repositorio de datos* podrá informar de anomalías sobre los datos enviados al usuario *entrada de datos*, a fin de que dicho usuario realice las tareas que crea conveniente para la subsanación de dichas anomalías.

Por otra parte, un *consultor de datos* sólo podrá consultar datos procedentes de un envío de datos una vez dentro de la ventana temporal establecida para la consulta de datos almacenados en el repositorio. Debe tenerse presente que el *consultor de datos* sí podrá consultar los datos previos, es decir, procedente de envíos cuya ventana temporal haya finalizado.

Gestionar subsistema repositorio de datos

Conjunto de funcionalidades mediante las cuales la entidad gestora podrá definir el funcionamiento del subsistema repositorio de datos. Entre ellas se establece la potestad de administrar el acceso del sistema a los distintos

usuarios *consultor de datos*, establecer el conjunto de datos que serán accesibles para las distintas áreas operativas del sistema, etc.

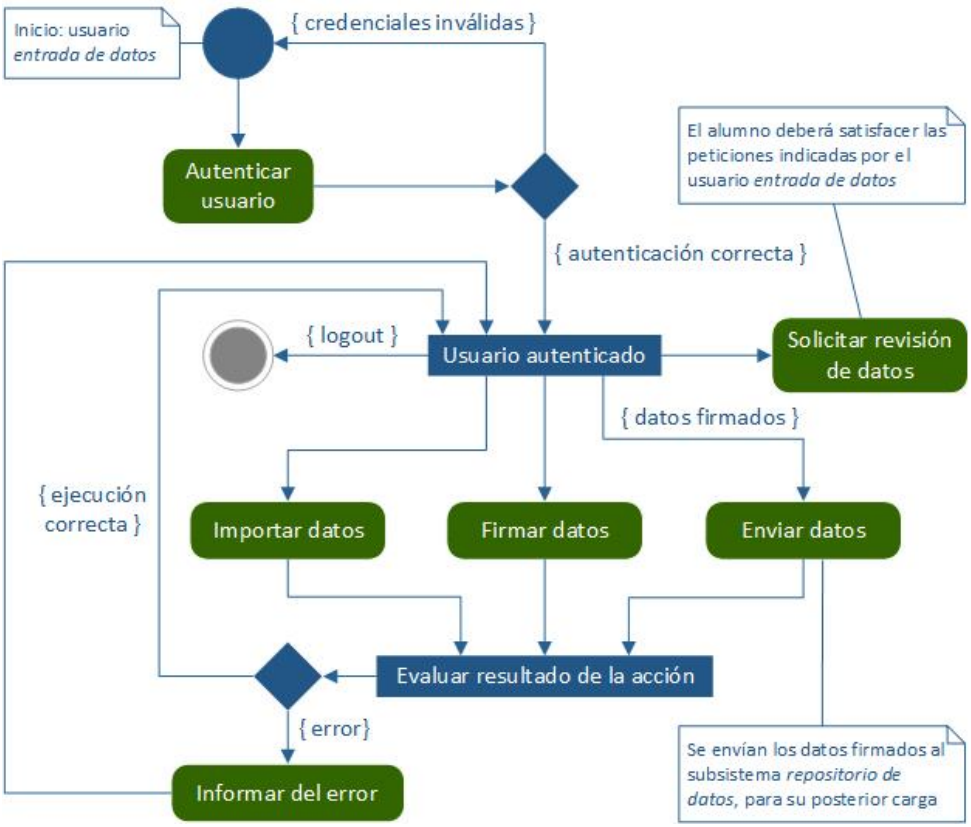
Diagramas de actividad

Esta sección pretende ofrecer una visión más clara sobre la operativa del sistema. Para ello se han incluido los diagramas de actividad referentes a cada uno de los dos subsistemas de que consta el sistema de información propuesto. Estos diagramas mostrarán de forma funcional la evolución en cuanto a actividad de los diversos subsistemas, de acuerdo a los casos de uso planteados con anterioridad.

Subsistema entrada de datos

Tal y como se ha comentado anteriormente, el subsistema *entrada de datos* es el encargado de proveer de información al subsistema *repositorio de datos*. Pese a ser de importancia capital, su operativa se restringirá a unas pocas ventanas temporales durante el curso académico, ventanas en las que se podrá realizar dicho trasvase de información entre subsistemas.

Ilustración 7. Diagrama de actividad del subsistema entrada de datos.



La Ilustración 7 muestra de forma general cómo se desarrolla la actividad de este subsistema. Tal y como se puede apreciar, el usuario principal de este sistema es el usuario *entrada de datos*. Dicho usuario deberá estar previamente autenticado para poder realizar cualquier tipo de operación en el sistema. Una vez autenticado, podrá realizar cualquier de las acciones permitidas para su rol. Dichas acciones se pueden englobar en dos grandes bloques:

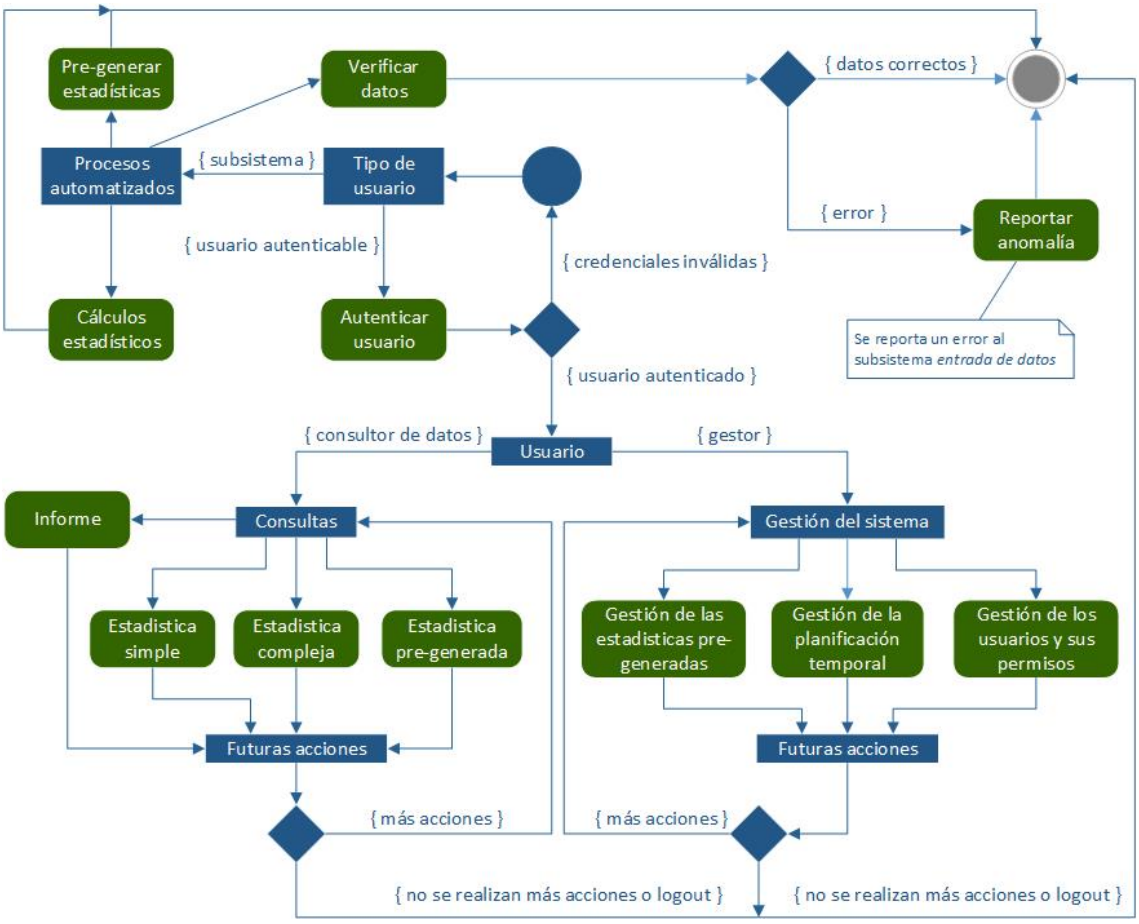
- Interacción con el subsistema *repositorio de datos*. En este contexto, el usuario *entrada de datos* tiene como objetivo principal la provisión de datos al subsistema *repositorio de datos*. Para ello deberá proceder, en primer lugar, a la importación de los datos en un formato que sea adecuado para su posterior carga en el subsistema repositorio de datos. Este procedimiento de importación puede comprender simplemente un proceso de modificación de los datos ya existentes, o bien implicar la definición de un subsistema completo que permita al usuario alumno introducir los datos requeridos en un formato adecuado para su importación de forma directa. Una vez los datos han sido importados, el usuario *entrada de datos* revisará su contenido, asegurando de esta forma la validez de los mismos. Una vez el usuario esté seguro de la validez de los datos, procederá a su firma. Con este procedimiento se pretende un doble propósito. En primer lugar congelar el bloque de datos a transmitir, permitiendo de esta forma un trabajo por lotes. En segundo lugar, se articula un mecanismo con el que autenticar la procedencia de los datos, asegurando de esta forma tanto su origen como su integridad. Una vez firmados, los datos podrán ser enviados al subsistema *repositorio de datos*, el cual se encargará de su posterior carga y almacenamiento.

- Interacción con el usuario *alumno*. Este segundo bloque de actividad comprende las acciones en las que se ve implicado el usuario *alumno*. Dichas acciones se reducen la a la solicitud de revisión de los datos al detectarse alguna anomalía en los mismos. Dicha anomalía puede reportarse en la revisión previa que el usuario *entrada de datos* realiza previa firma de los datos, o bien remitirse desde el subsistema *repositorio de datos* al proceder a la carga de los datos proporcionados.

Subsistema repositorio de datos

El subsistema repositorio de datos concentra la mayor parte de la funcionalidad del sistema, habida cuenta que su principal propósito es la provisión de un conjunto amplio de datos para su consulta por parte de la comunidad de investigadores interesada en ellos.

Ilustración 8. Diagrama de actividad del subsistema repositorio de datos.



La Ilustración 8 muestra de forma general cómo se desarrolla la actividad de este subsistema. Tal y como se puede apreciar, este subsistema consta de actividades propias de varios usuarios: consultor de datos (investigador), gestor y el propio subsistema. A continuación se ofrece un detalle sobre dichas actividades de acuerdo al usuario principal de las mismas.

- Subsistema. Este bloque de actividad engloba a todas aquellas acciones que se realizan de forma autónoma desde el propio subsistema. En concreto dichas actividades serán:_
    - Verificación de los datos proporcionados desde el subsistema *entrada de datos*. Cada vez que un usuario del

subsistema *entrada de datos* envíe datos firmados al subsistema repositorio de datos, éste último procederá a verificar la integridad de los datos y cotejar la correcta procedencia de los mismos, de acuerdo a la firma provista. Una vez certificada la procedencia de los datos, procederá a verificar el formato de los datos y su completa provisión. Una vez completada la verificación de la sintaxis de los datos provistos se procederá a su carga. Si cualquiera de estas acciones fallara, se notificará de este hecho al usuario *entrada de datos* fuente de la información proporcionada para que subsane en la medida de sus posibilidades la anomalía detectada.

- Pre-generación de estadísticas. Tal y como se ha comentado con anterioridad, el sistema dispondrá de forma permanente de un conjunto de estadísticas, correspondientes a los datos más solicitados. La disponibilidad de estas estadísticas permitirán al sistema ofrecer un mejor tiempo de respuesta al tiempo que ofrecerá a los consultores de datos una mejor experiencia de usuario. De esta forma, el subsistema procederá a pre-generar estas estadísticas de forma periódica de acuerdo con los datos que hayan sido demandados por los distintos consultores que operan en el sistema.

- Cálculos estadísticos. Esta actividad se realizará de forma periódica con el objetivo de cuantificar el uso de los distintos datos puestos a disposición de los consultores, así como para generar datos sobre el propio uso del sistema. Con ello se pretende la mejora constante del sistema, al tiempo que se permiten actividades como la indicada en el apartado b) pre-generación de estadísticas.

Para las actividades referentes al resto de usuarios, el usuario deberá estar previamente autenticado. Una vez autenticado, podrá realizar cualquier de las acciones permitidas para su rol. De acuerdo con el tipo de usuario, dichas acciones serán:

- Consultor de datos. Este usuario podrá realizar de forma indistinta cualquiera de las acciones de consulta previstas en el sistema. En concreto, podrá realizar consultas sobre los datos almacenados, sean éstas pre-generadas por el sistema, simples (es decir, definidas por el usuario e involucrando 2 variables) o complejas

(definidas por el usuario e involucrando más de 2 variables). También podrá solicitar informes que recojan un número deseado de estadísticas. Dichos informes, a diferencia de las estadísticas, vendrán firmados por el sistema para certificar su origen e integridad.

- Gestor. Este es el usuario principal de una serie de actividades relacionadas con la operativa del propio sistema de información. En concreto dichas actividades se agrupan en tres grandes bloques:
    - Gestión de las estadísticas pre-generadas. En concreto, el gestor definirá los criterios (temporales, operativos, etc.) bajo los cuales se generarán las distintas estadísticas.
    - Gestión de las ventanas temporales. Estas actividades están asociadas a la definición y mantenimiento de las distintas ventanas temporales que definirán. Por ejemplo establecerán los periodos temporales en los que los usuarios entrada de datos podrán enviar datos para su posterior carga en el sistema. También podrán establecerse ventanas temporales durante las cuales los consultores no puedan acceder a los datos, o bien lo hagan a un subconjunto de los mismos.
    - Gestión de los usuarios y sus permisos. Este bloque de actividades hace referencia a las acciones que podrá llevar a cabo el gestor para establecer el rol de los distintos usuarios del sistema, así como los permisos asignados a cada uno de los roles definidos.

Modelo de datos

En este apartado se define el modelo de datos a emplear. Este modelo se ha estructurado de acuerdo a dos paradigmas diferenciados:

1. Modelo de datos genérico. Con ello se pretende definir un modelo de datos general, sin particularizar dicho modelo a un paradigma de implementación concreto y sin tener en cuenta el sistema gestor de base de datos sobre el que se levantaría dicha implementación.
2. Modelo de datos particularizado. Con ello se pretende ofrecer una posible implementación del modelo de datos, empleando para ello el modelo entidad-relación y un sistema gestor de base de datos concreto.

Los siguientes subapartados se encargan de exponer los dos puntos anteriormente citados.

Especificación del modelo de datos

En este apartado se pretende ofrecer la especificación del modelo de datos, es decir, una definición de dicho modelo independiente de la tecnología finalmente usada para su implementación.

Existe una restricción no textual que es común a todos los diagramas y que por tanto debe tenerse en cuenta en todos los diagramas. Dicha restricción establece que todo aquel dato susceptible de representarse en múltiples idiomas, estará ligado al idioma establecido por el *UsuarioRegistrado* implicado en la operación con el sistema de datos.

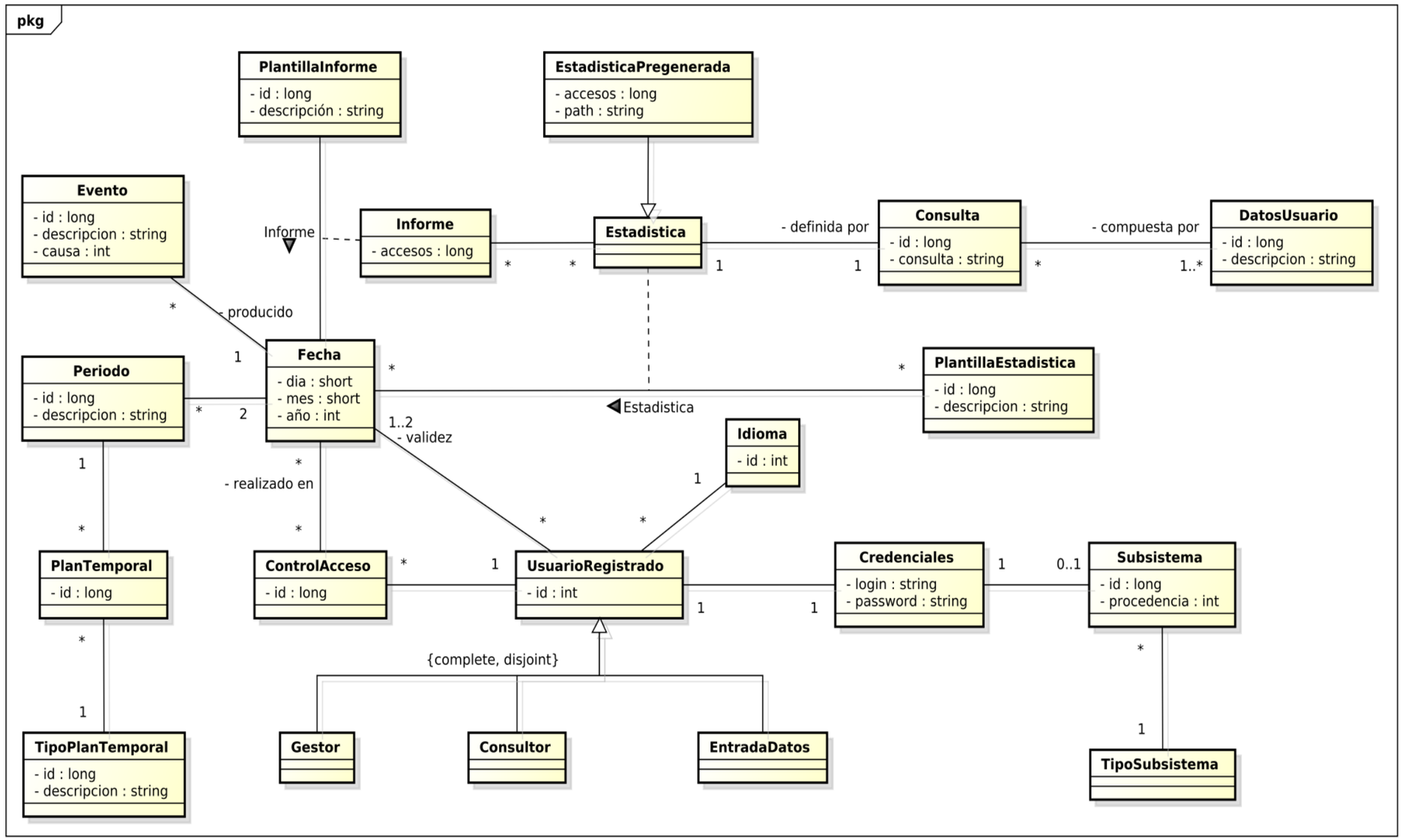
Debe tenerse en cuenta que el diseño del modelo de datos se ha hecho bajo la premisa de generalidad, es decir, intentando en todo momento abarcar tanto los requerimientos actuales como los futuros. De esta forma, cualquier dato que venga definido por un rango de valores textuales finito se ha especificado dentro del modelo de datos como una dupla valor-descripción. Este mecanismo permite ampliar el rango de posibles valores del dato o bien alterar su descripción, situaciones muy frecuentes en los sistemas de información con una alta dependencia del modelo de datos. Un ejemplo de este proceder podría ser la codificación del dato "Nivel de estudios". Este dato, inicialmente podría proponer una codificación en base a tres niveles: "Estudios pre-universitarios, estudios universitarios y doctorado". Sin embargo, en un futuro podría desearse una mayor precisión, separando doctorado y master, o bien un cambio en la manera de denominar cada uno de los niveles de estudio.

En las siguientes figuras se detallan los diagramas de clases correspondientes a distintas partes del modelo de datos, de acuerdo a la tipología de los datos a los que hacen referencia.

Núcleo del sistema

Diagrama de clases

Ilustración 9. Diagrama de clases referente al núcleo del sistema INUDIS.



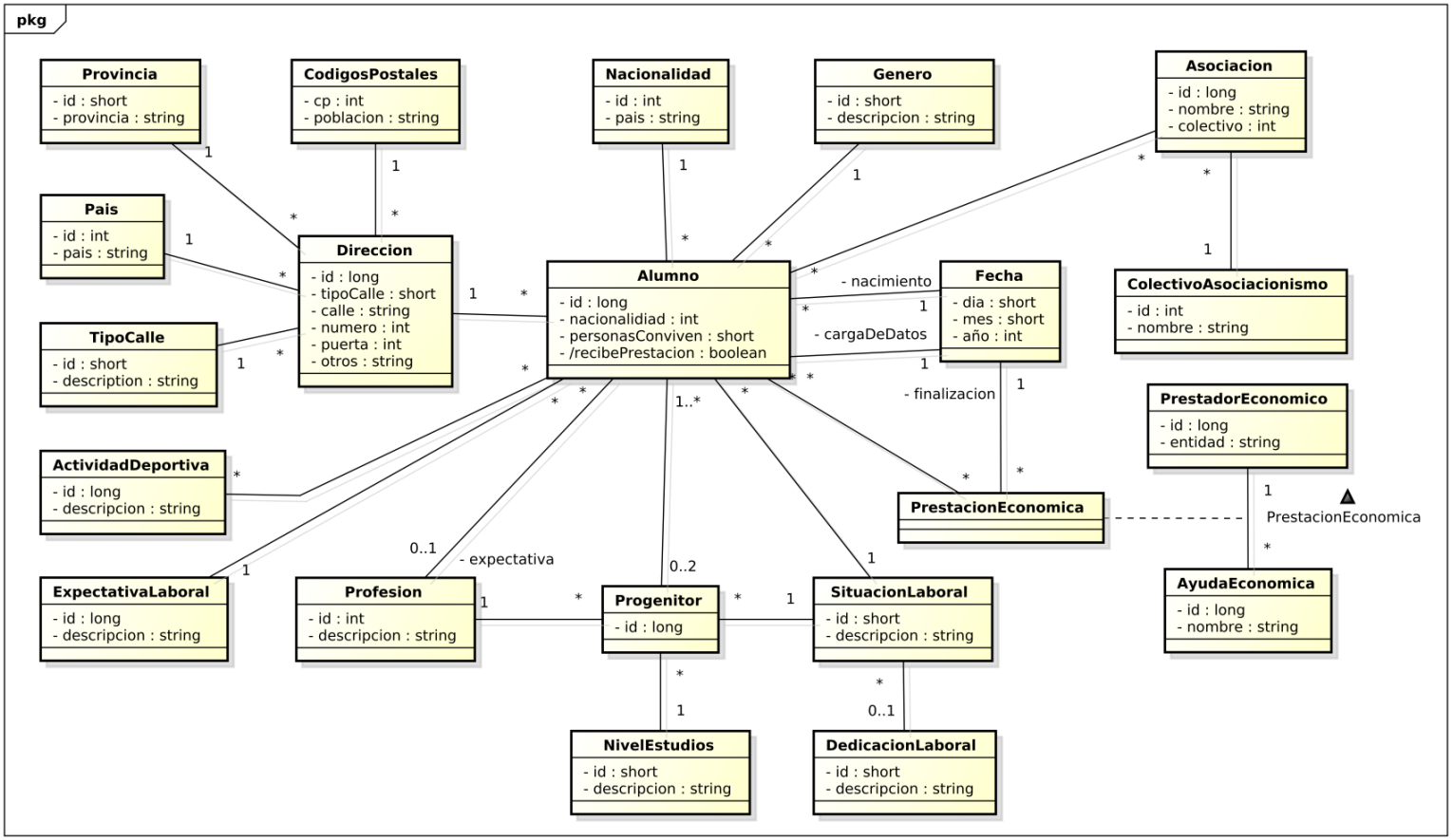
Restricciones no textuales

- En todo Periodo, la Fecha de inicio será anterior (o igual) a la de finalización.
- Todos los datos recogidos en los distintos objetos estarán en el Idioma establecido en *UsuarioRegistrado*.

Conceptos personales relacionados con el alumno

Diagrama de clases

Ilustración 10. Diagrama de clases referente a los conceptos personales relacionados con el alumno.



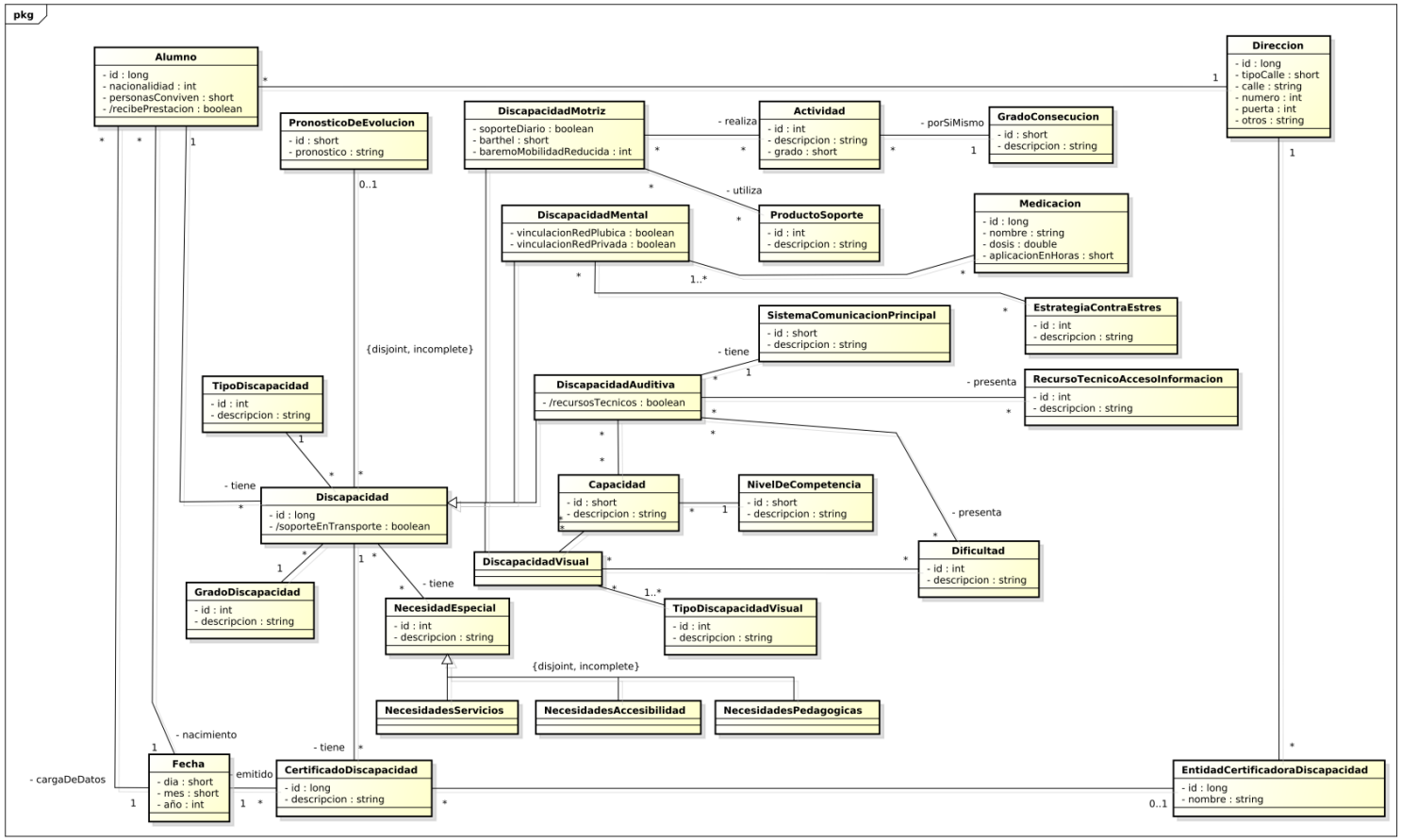
Restricciones no textuales

- La *Provincia* de una *Dirección* debe corresponderse con la vinculada al Código Postal de dicha Dirección.
- La *Provincia* asociada a una *Dirección* debe existir en el *País* en el que se enmarca dicha *Dirección*.
- La *Fecha* de nacimiento del alumno debe ser anterior en como mínimo 18 años a la *Fecha* de carga de los datos (cargaDeDatos).
- El atributo derivado *recibePrestacion* de la clase *Alumno* será cierto cuando exista alguna asociación entre *Alumno* y *PrestacionEconomica*.

Datos introducidos por el alumno acerca de su condición

Diagrama de clases

Ilustración 11. Diagrama de clases referente a los datos introducidos por el alumno acerca de su condición



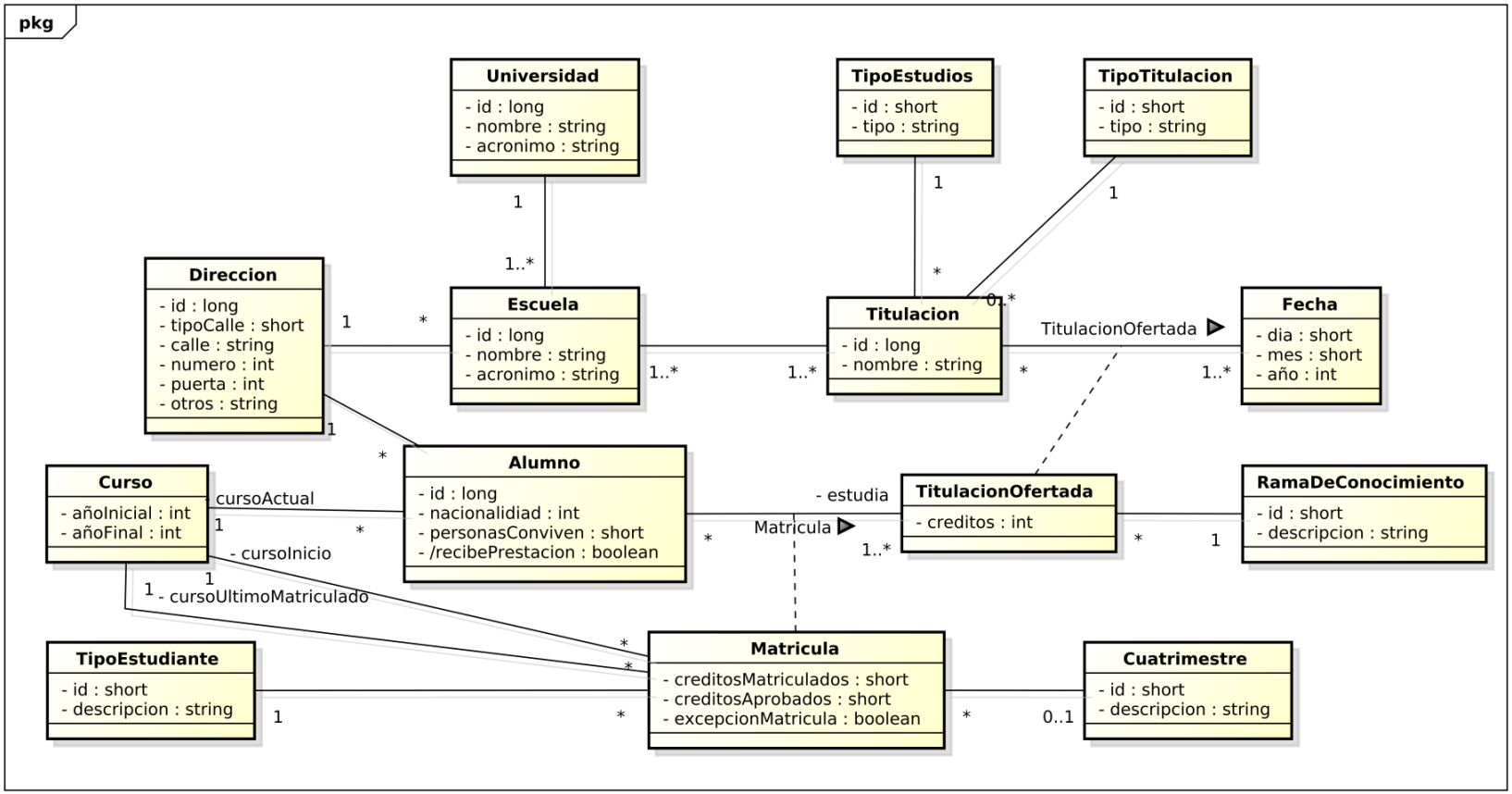
Restricciones no textuales

- La Fecha de emisión de un certificado no puede ser anterior a la de nacimiento del Alumno al que está vinculado.
- Una Discapacidad Visual y una Discapacidad Auditiva no pueden compartir una misma Capacidad.
- Una Discapacidad Visual y una Discapacidad Auditiva no pueden compartir una misma Dificultad.

Conceptos académicos relacionados con el alumno

Diagrama de clases

Ilustración 12. Diagrama de clases referente a los conceptos académicos relacionados con el alumno.



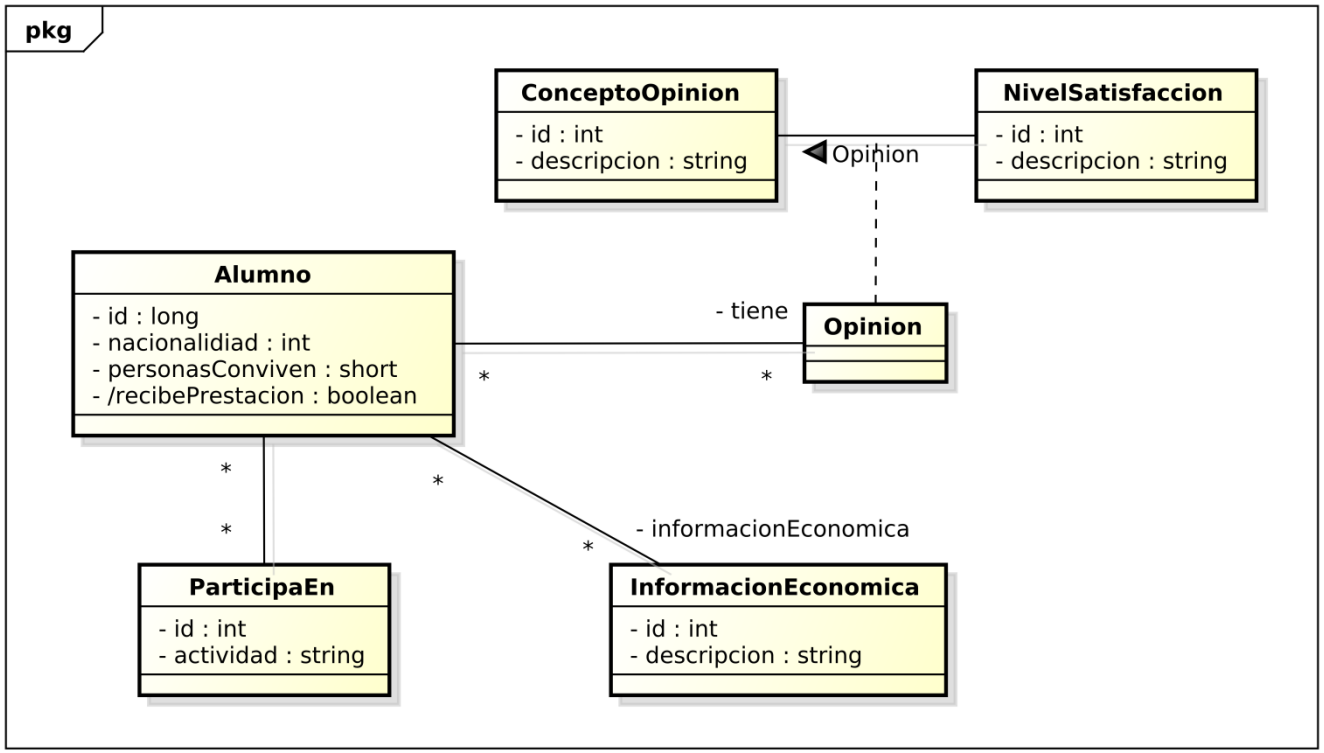
Restricciones no textuales

- El *Curso Actual* de un *Alumno* debe ser igual o posterior al *Curso* de *Inicio* de cualquiera de los estudios en los que dicho *Alumno* está implicado.
- El último curso matriculado (cursoUltimoMatriculado) debe ser igual o posterior al curso de inicio (cursoInicio).
- El número de créditos aprobados (creditosAprobados) en una Matrícula debe ser igual o inferior al número de créditos matriculados (creditosMatriculados).
- El año de la Fecha en la que se oferta una *TitulacionOfertada* será anterior o igual al indicado en el atributo *añoInicial* de los *Cursos* asociados a la *Matrícula* (cursoActual, cursoInicio, cursoUltimoMatriculado).
- Los créditos de una T*itulacionOfertada* deben ser superiores a los créditos matriculados (creditosMatriculados) de toda *Matricula* a la que se asocie dicha titulación.

Conceptos participativos relacionados con el alumno

Diagrama de clases

Ilustración 13. Diagrama de clases referente a los conceptos participativos relacionados con el alumno.



Restricciones no textuales

Ninguna a destacar.

Diseño del modelo de datos

Sistema gestor de base de datos

La elección de un sistema gestor de base de datos (SGBD) es una pieza clave de cualquier implementación de un modelo de datos. Se han establecido tres criterios con los que permitir una mejor selección del sistema gestor de base de datos en el proyecto INUDIS: 1) carga estimada del sistema, 2) coste del sistema gestor de base de datos y 3) capacidades y soporte del SGBD. Los SGBDs candidatos son, a priori, los siguientes: MySQL , PostgreSQL, Microsoft SQL Server y Oracle DB. El criterio para establecer estos productos como punto de partida es su situación predominante en el mercado de los SGBDs.

De acuerdo al documento de análisis de requerimientos, se estima que la carga sobre el sistema gestor de base de datos se concentrará en las actividades realizadas por los usuarios de tipo consultor, cuyo número se considera reducido (del orden de 100). Con estos datos, cabe esperar un número de accesos simultáneos muy reducido, lo que permite a priori el uso de cualquier sistema gestor de base de datos de entre los candidatos.

Otro factor determinante para la elección del SGBD es el número de registros esperable por tabla. En este sentido, el modelo de datos asume que habrá tablas muy cargadas de registros, puesto que se deseará mantener todo dato que haya sido previamente introducido. Como agravante, se considera que las cargas de datos serán disociadas, es decir, no se podrán relacionar datos entre periodos de carga distintos. Esto conlleva un claro crecimiento monótono del volumen de datos almacenados por el SGBD. Este tipo de crecimiento monótono en el número de registros podría dar al traste con el rendimiento de cualquier SGBD, que puede verse obligado a reservar tablas temporales de gran tamaño e invertir un tiempo considerable en la resolución de las pertinentes consultas. Es por eso que se establecerán dos bases de datos diferenciadas, una con los datos de los últimos 10 años y otra con los datos anteriores a dicha fecha. Bajo esta premisa se estima que la base de datos con la información más reciente, cuyo acceso se considera prioritario, almacenará como máximo un orden de magnitud de millones de registros. Esta cifra es asumible cualquiera de los SGBDs considerados.

Por coste, mySQL y postgreSQL son productos que pueden emplearse de forma gratuita, frente Microsoft SQL Server y Orable DB que son productos con

licencia comercial. De acuerdo con los requerimientos del proyecto, el coste es un factor a tener en cuenta, por lo que se descartará el uso de productos comerciales para así evitar el pago de las pertinentes licencias.

El soporte de mySQL y postgreSQL es muy notable, si bien en términos de documentación y herramientas de desarrollo disponibles, mySQL tiene una ligera ventaja frente apostgreSQL. Habida cuenta que la carga no es factor crítico en el diseño de datos actual, se ha decido seleccionar mySQL como SGBD.

Modelo de datos entidad-relación (ER)

El presente apartado presenta una posible implementación en mySQL del modelo de datos según el paradigma de diseño de entidad-relación. Para ello se han tenido en cuenta los distintos diagramas de clases anteriormente presentados. De igual forma, las restricciones no textuales citadas para los diferentes diagramas de clase serán de aplicación en el modelo de datos aquí presentado.

Ilustración 14. Modelo de datos del núcleo del sistema según el paradigma entidad-relación (mySQL).

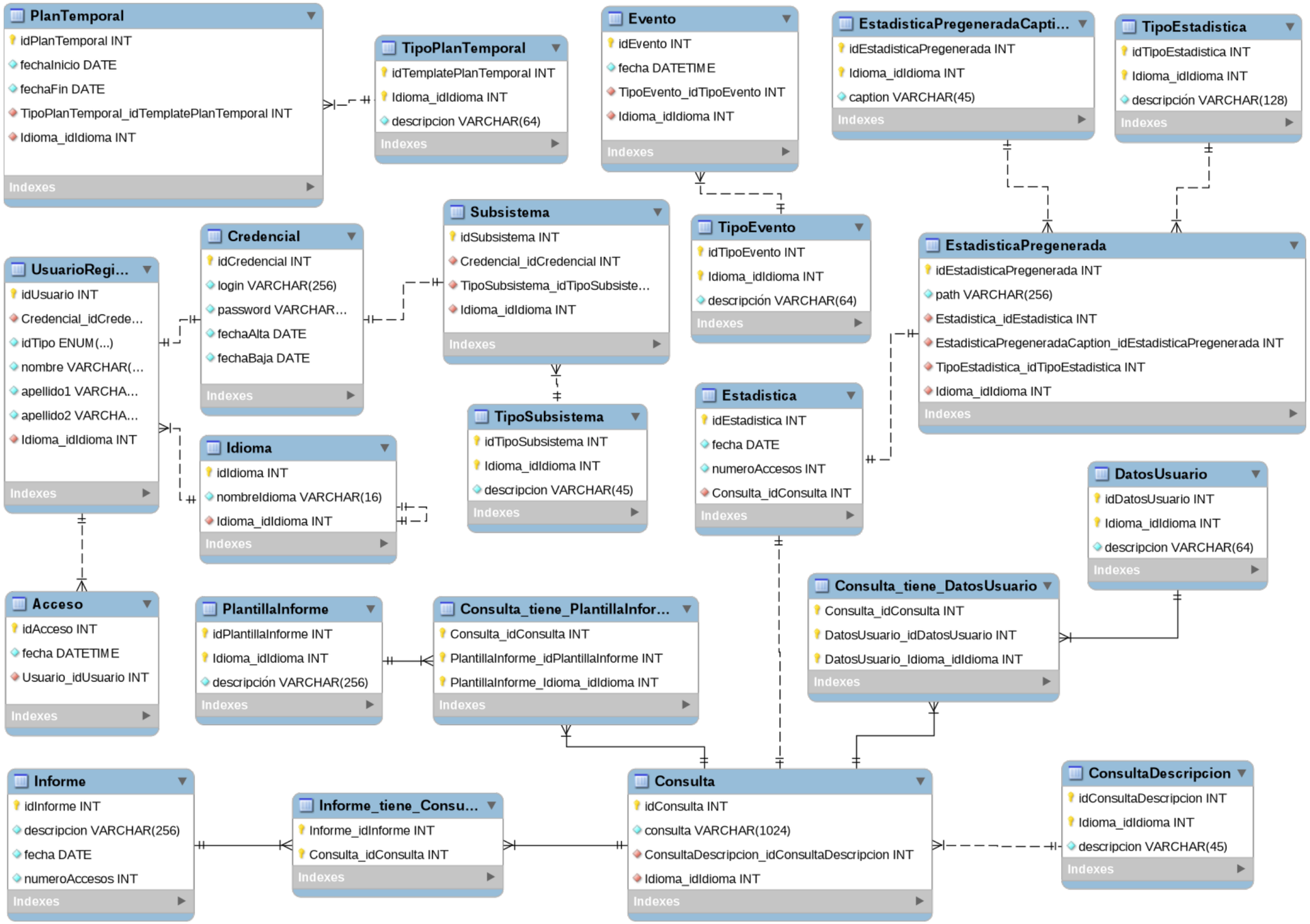


Ilustración 15. Modelo de datos referente a los conceptos personales, académicos y participativos del alumno según el paradigma entidad-relación /mySQL).

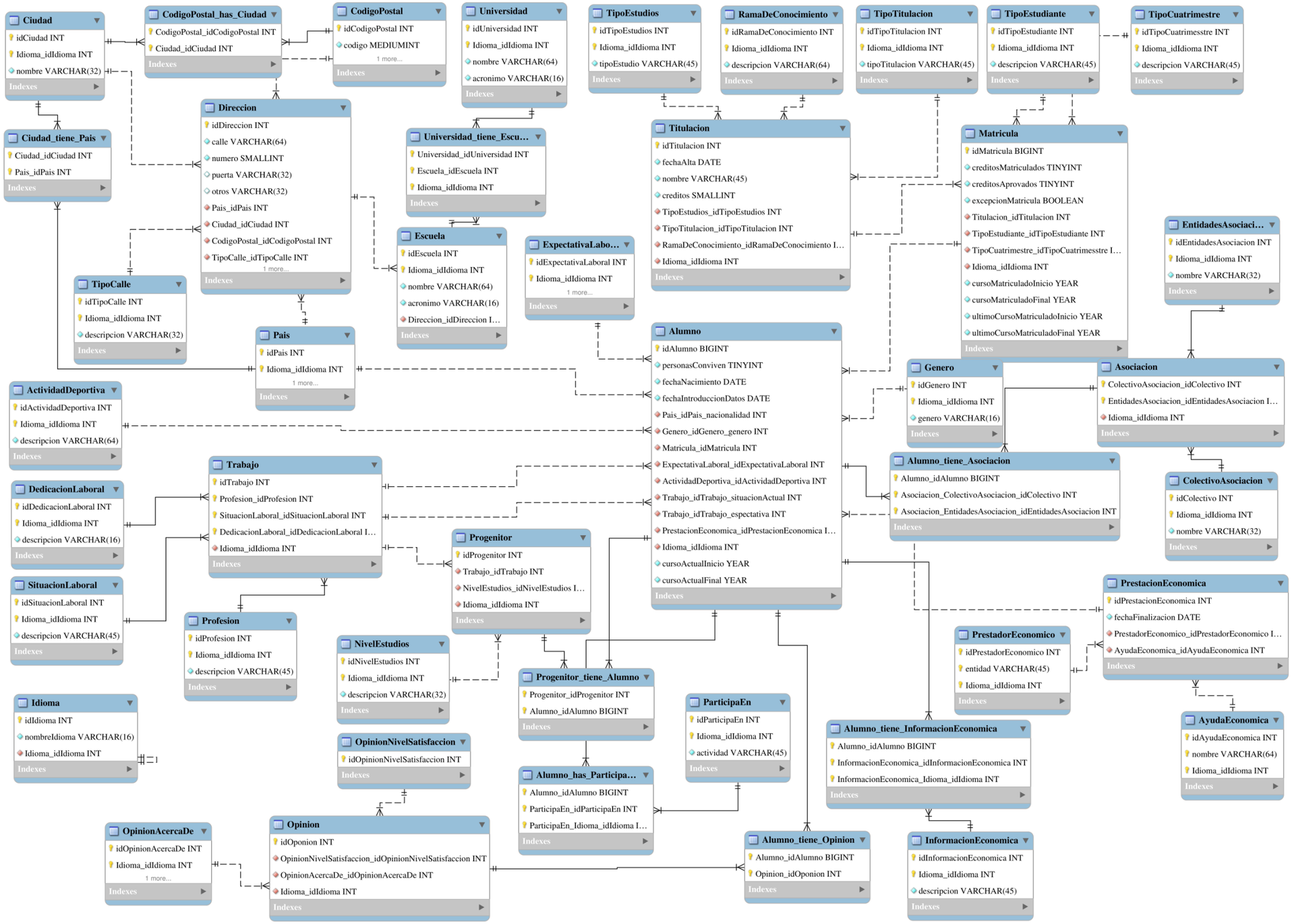
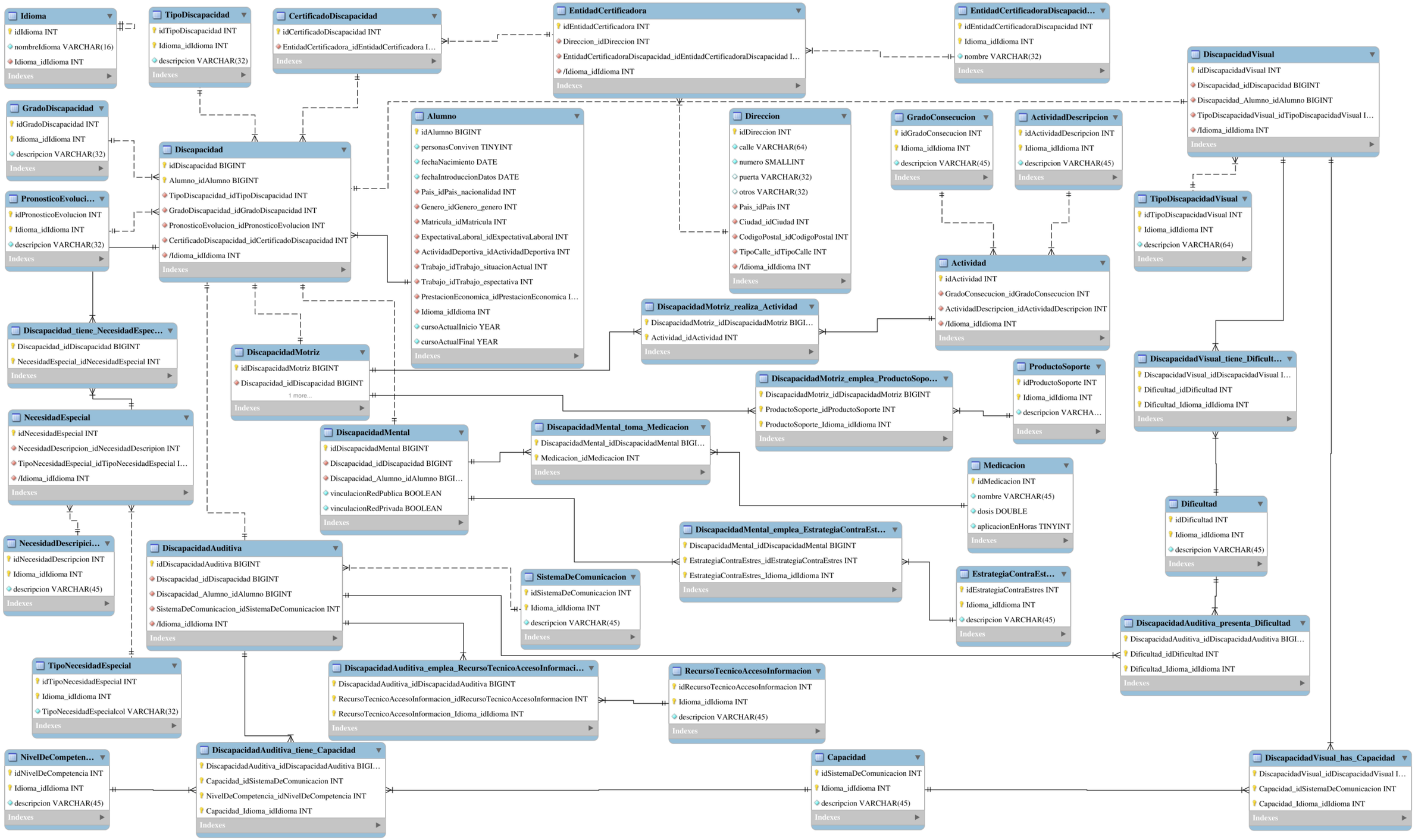


Ilustración 16. Modelo de datos referente a la condición del alumno según el paradigma entidad-relación (mySQL).



CONCLUSIONES

El objetivo general del proyecto de definir un sistema global de gestión de la información estadística relativa al alumnado con discapacidad aplicable en las universidades públicas españolas se ha logrado cumplir satisfactoriamente tras los análisis académicos, legales y técnicos. Nótese que realmente se ha definido un sistema de gestión para todo el alumnado universitario, incluyendo a los alumnos con discapacidad.

El análisis de los requerimientos legales necesarios para la gestión de los datos académicos del alumnado de las universidades españolas ha demostrado la viabilidad del sistema si se cumplen un conjunto de preceptos. Teniendo como marco de trabajo la Ley de Protección de Datos Personales, el análisis establece que los datos de salud del alumnado son los más sensibles en su compartición y gestión (considerados de nivel de seguridad alto). Estos datos son fundamentales en el caso de considerar los factores relativos a la discapacidad en los estudios de los investigadores. Por lo tanto es imperativo disociar los datos relativos a la identidad del alumnado del resto de datos en su transmisión, almacenamiento y gestión para cumplir la legislación.

El análisis curricular del perfil de los estudiantes universitarios ha permitido identificar y categorizar los datos clave que maximizan la información sobre el alumnado. Este proceso se ha llevado a cabo teniendo en cuenta criterios interuniversitarios, adoptando como propios cuando ha sido posible consensos de hecho. Se han identificado 119 datos a incorporar en el sistema de gestión de información, agrupados en 7 categorías: datos personales, académicos, económicos, capacidades, necesidades, participación y calidad. La suma de todos ellos ofrece una visión amplia y detallada de la situación de los alumnos con discapacidad en la universidad.

El estudio propone un método para identificar de forma unívoca a un estudiante dentro del sistema universitario español. Este procedimiento inicialmente no se había previsto, ya que no es trivial detectar el problema si no se analiza a fondo el sistema de gestión y matrícula universitario. El problema reside en que existe una amplia variedad de procedencias entre el alumnado. Existiendo por lo tanto múltiples opciones para la identificación personal de un alumno: NIF, NIE, pasaporte, etc.

La premisa impuesta por el análisis legal de disociar los datos vinculados a la identidad del alumnado del resto se ha resuelto mediante un protocolo de agregación anónima de datos que garantiza estrictamente el cumplimiento de

la ley. El proceso se fundamenta en que las universidades generan identificadores unívocos cifrados para cada estudiante; las universidades comparten sus datos con el sistema de información facilitando el identificador cifrado (que el sistema no puede asociar a ningún alumno, pero sí le permite cruzar información de distintas universidades); y el sistema de información almacena los datos usando un segundo identificador cifrado (no hay datos que identifiquen a un estudiante). Por lo tanto ni los centros de investigación, ni las universidades, pueden asociar los datos a ningún alumno cuando solicitan informes al sistema de información. Informes que además contienen datos agregados. Los datos están protegidos pero pueden usarse.

El núcleo operativo del sistema de información reside en la base de datos que contiene todos los registros del alumnado. Se ha formulado de forma extensa su definición para garantizar su correcto funcionamiento. Además de las premisas académicas y legales se han contemplado requisitos de seguridad de la información, eficiencia de su gestión, minimizar costes económicos, optimizar su mantenimiento, alta escalabilidad y portabilidad.

Para llevar a cabo el diseño global del sistema ha sido necesario realizar también un análisis técnico gracias al cual se han definido las especificaciones técnicas del sistema. A su vez, en base a estas especificaciones se ha diseñado el sistema de información que refleja la situación del alumnado con discapacidad en la universidad.

Las premisas básicas para el diseño han sido en primer lugar la universalidad ya que los datos recogidos son de todos los estudiantes y no solo los del alumnado con discapacidad. El tratado posterior de los datos es el que permite realizar los análisis adecuados para conseguir una visión global y real de la situación. La segunda premisa ha sido la escalabilidad. El sistema puede ser implementado para un grupo reducido de universidades como para todas ellas, pudiéndose plantear también una inclusión paulatina de estos organismos. Por último la implantación es genérica, es decir, que el sistema puede ser implementado de forma factible en cualquier universidad española. Todas estas premisas son retos importantes que han sido también superados con éxito.

El sistema contempla la interacción de los usuarios, los equipos, las comunicaciones y los datos. La infraestructura necesaria engloba a equipos y sistemas de comunicaciones. Los datos, tanto académicos como de soporte de gestión, son los elementos que aportan valor al sistema.

El servicio de información se articula alrededor de las universidades, los centros de investigación y la entidad gestora. Las universidades son la fuente de información del servicio ya que aportan los datos académicos de su

alumnado asegurándose de su veracidad. Los investigadores y organismos interesados reciben datos estadísticos agregados sobre el alumnado de las universidades. A pesar de tener acceso a las bases de datos, nunca se podrá identificar datos personales de estudiantes individuales, puesto que en las fases iniciales se han disociado los datos académicos de los datos personales. La entidad gestora debe ser en todo caso una administración pública.

Todas las comunicaciones entre los miembros del sistema de información se realizan de forma segura, mediante los protocolos escogidos a tal efecto, con lo que quedan garantizadas tanto la autenticación mutua de los comunicantes como la privacidad e integridad de los datos transmitidos.

La topología del sistema es del tipo Screening Subnet Firewall implementada con dos cortafuegos, cuatro servidores y una cabina de discos. Por motivos de seguridad la red interna de la Entidad Gestora se divide en un segmento interior seguro protegido por cortafuegos y un segmento exterior de acceso para las universidades y organismos. En el segmento interior o red privada, se ubican los servidores principales de la Entidad Gestora. Estos servidores contienen la base de datos académicos y la Autoridad Certificadora. La Autoridad Certificadora es la encargada de cifrar y firmar los datos. La cabina de discos es la responsable de mantener copias de seguridad de la base de datos académicos y de los certificados.

El sistema se ha diseñado de tal forma que cumpla con un conjunto de reglas. En primer lugar el sistema debe, incluir un conjunto exhaustivo de datos que aporten funcionalidad al sistema, no limitar el número de estudios cursados simultáneamente siendo entregados los datos del alumno en cada centro correspondiente y los investigadores y organismos interesados deben tener acceso a los datos pero sin poder relacionarlos con alumnos concretos. Los datos solo podrán ser relacionados con el centro de estudios para así poder detectar posibles inconsistencias. En cualquier caso, la entidad gestora puede limitar el acceso a ciertos datos si nos los considera apropiados para los fines de la entidad solicitante. Los procesos de introducción de los datos por parte de los alumnos, de verificación de los mismos por los responsables de la entrada de datos en el centro en el que dichos alumnos cursan sus estudios, así como de su posterior carga en el repositorio de datos estarán acotados temporalmente de acuerdo a una planificación establecida por la entidad gestora del sistema. Sólo un conjunto de usuarios por centro, habilitados a tal efecto, tendrán acceso a los datos identificativos de los alumnos y sólo un usuario por centro podrá firmar los datos, dando validez a los mismos.

En el diseño del sistema se han tenido en cuenta requerimientos de experiencia de usuario, de rendimiento, operacionales y de entorno. Se ha

diseñado también de forma exhaustiva la base de datos académicos, teniendo en cuenta, los usuarios, los subsistemas, los casos de uso principales, los diagramas de actividad y el modelo de datos.

Como aspectos a destacar, cabe decir que a nivel técnico se presenta una solución completa. A partir del diseño presentado es posible implementar el sistema siendo totalmente operativo. Pero para que realmente se obtengan los resultados deseados es imprescindible una voluntad política real de los organismos pertinentes (Conferencia de Rectores de Universidades Españolas, Agencia Nacional de Evaluación de la Calidad y Acreditación, etc.) que apoyen y promuevan su implantación.

Este proyecto se ha planteado de una forma universal e inclusiva. A nivel teórico el trabajo está hecho. A nivel práctico, todavía no es una realidad. Ello conllevaría la implementación técnica, el compromiso político, la colaboración efectiva entre las distintas universidades y el mantenimiento sostenido en el tiempo del sistema.

Los beneficios serian muchos: mayor conocimiento de la situación real de la comunidad universitaria en cuanto a la discapacidad (problemas, necesidades, satisfacción), promoción y generación de conocimiento científico sobre la materia al proveer a los investigadores de datos reales, veraces y actuales, toma de decisiones por parte de la dirección de las universidades basadas en datos estadísticos fiables sobre su accesibilidad, creación de políticas y estrategias efectivas a nivel estatal gracias a la disponibilidad de información global, posibilidad de proveer al tejido asociativo de datos para llevar a cabo evaluaciones de estado en sus respectivos ámbitos, sensibilización de la sociedad y del sector empresarial sobre la igualdad de oportunidades, informar y sensibilizar a los docentes sobre la diversidad que existe en sus aulas y ofrecer a los propios estudiantes con discapacidad información de contexto sobre su realidad en la universidad, por mencionar algunos de ellos.

BIBLIOGRAFÍA

(DSS), D. S. (s.f.). Obtenido de http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf

Boletín Oficial del Estado, R. D. (2008). *Núm. 17, Sábado 19 enero 2008*. Recuperado el 2013, de BOE: http://www.boe.es/boe/dias/2008/01/19/pdfs/A04103-04136.pdf

Cryptography, R. f.-W. (s.f.). Obtenido de http://csrc.nist.gov/groups/ST/toolkit/documents/SP800-56Arev1_3-8-07.pdf

curves, M. r. (s.f.). Obtenido de http://www.nsa.gov/ia/_files/nist-routines.pdf

Daniel Guasch, M. H. (2012). *Evaluación de la implementación de los principios de igualdad de oportunidades y accesibilidad universal en los planes de estudios de los títulos de grado de las universidades españolas*. Observatorio Universidad y Discapacidad.

Daniel Guasch, P. D. (2013). *La responsabilidad social universitaria y discapacidad*. Observatorio Universidad y Discapacidad.

Daniel Guasch, S. B. (2010). *Estudio sectorial por comunidades autónomas de la accesibilidad del entorno universitario y su percepción: Observatorio Universidad y Discapacidad*. Observatorio Universidad y Dsicapacidad.

Fundación Universia. (2011). *Universidad y Discapacidad, estudio sobre el grado de inclusión del sistema universitario español respecto de la realidad de la discapacidad*. Fundación Universia.

Gobierno de España. (1999). *Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal*. Recuperado el 2013, de Agencia Estatal Boletín Oficial del Estado: http://www.boe.es/buscar/doc.php?id=BOE-A-1999-23750

Open SSL Team. (s.f.). *Open SSL Project*. Recuperado el 2013, de Cryptography and SSL/TLS Toolkit: http://www.openssl.org/

ANEXOS

El apartado de Anexos se ha dividido en dos partes. La primera contiene los anexos de carácter legal y la segunda contiene los anexos de carácter técnico. Debido a la extensión de los anexos técnicos éstos se publican en el Anexo II en un documento aparte.

ANEXO I.

Modelo de recogida de datos: leyendas.

En cumplimiento de la LO 15/99 de Protección de datos de Carácter Personal , le informamos que los datos personales facilitados por usted serán incorporados en un fichero responsabilidad de <Organización>, denominado <XXXXXXXXX>, para finalidades relacionadas con el proyecto Sistema global de información sobre la discapacidad en la universidad.

Sus datos podrán ser facilitados al <OGR> como encargado del tratamiento y gestor del proyecto para que pueda proceder a las correspondientes actividades de tratado de los mismos. La <Organización> establece un acuerdo de cesión de los datos y de confidencialidad con el Encargado de tratamiento de los datos u otros gestores terceros, para que puedan proceder al tratado de los mismos o, en su caso, para que mantengan la confidencialidad y el secreto profesional legalmente aplicable.

En cualquier caso y momento, tanto de forma global como parcial, le informamos que usted puede ejercer delante la <Organización> su derecho al acceso, rectificación, cancelación y oposición de sus datos al tratamiento anteriormente mencionados. Para ejercer este derecho, puede enviar un correo electrónico a la dirección <XXXXXXXXX>, indicando Referencia LOPD y el contenido y alcance de su solicitud.

Modelo de protección de datos de OGR como encargado del tratamiento de datos de las universidades.

En ……, a…… de…….. de 20…. .

Reunidos

De una parte, <Universidad> con NIF <XXXXXXX> y domicilio en ……, representada por ……... con DNI ……. en calidad de …… .

De la otra parte, <OGR> con NIF <XXXXXXX> y domicilio en ……, representada por …….. con DNI ……. en calidad de …… .

Exponen

Que la <OGR> ha contratado con la <Universidad>, la prestación del servicio <Tipo de servicio> , al amparo del /os contrato/s suscrito/s por ambas partes.

Que para llevar a cabo estos servicios contratados será necesario que el <OGR>, en su calidad de encargado del tratamiento, acceda a datos de carácter personal incluidos en los ficheros facilitados propiedad de <Universidad>.

Que por este motivo y en cumplimiento del artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre de Protección de Datos de Carácter Personal , las dos partes acuerdan libremente regular el acceso y el tratamiento de datos de conformidad con las siguientes cláusulas

Cláusulas

PRIMERA. – Que <Universidad> como responsable de los ficheros, conoce que ha de proceder a su inscripción en el Registro General de la Agencia Española de Protección de Datos, y cumplir con todos los requisitos legales para la recogida y tratamiento de los datos incluidos en los mismos. Así mismo conoce que ha de adoptar todas las medidas técnicas y organizativas necesarias para garantizar la seguridad de los datos de carácter personal establecidas en el Título VIII del Real Decreto 1720/2007 de 19 de Enero.

SEGUNDA. – Que el acceso por parte del <OGR> a los dicheros de <Universidad> , será única y exclusivamente para gestionar los servicios encargados. <OGR> se compromete a no divulgar, ni comunicar a terceros la información obtenida como consecuencia de esta relación contractual; ni tan solo para su conservación, excepto que este supuesto quede fijado en alguna de las siguientes cláusulas. Además, el <OGR> se compromete a tratar los datos conforme a los términos exigidos en la normativa aplicable.

TERCERA. - <OGR> implementará las medidas técnicas y organizativas necesarias que garanticen la seguridad e integridad de los datos de carácter personal incluidos en los ficheros y que eviten su alteración, pérdida, tratamiento y acceso no autorizados, teniendo en cuenta el estado de la tecnología, la naturaleza de los datos almacenados, y los riesgos del hecho de estar expuestos, ya provenga de la acción humana, del medio físico o natural. Las medidas de seguridad mencionadas son las determinadas en el Título VIII del Real decreto 1720/2007 de 19 de enero.

QUARTA. - <OGR> se compromete al secreto profesional respecto a los datos incluidos en los ficheros, obligación que subsistirá aún después de finalizar sus relaciones con <Universidad> . Únicamente accederán a los datos personales el servicio técnico y personal que tengan necesidad de acceder a ellos para llevar a cabo sus funciones en relación a los servicios. A todos ellos se les advertirá del carácter confidencial de la información y de su responsabilidad en caso de divulgarla.

QUINTA. – El/los signatarios autorizan a <OGR> , a incorporar los datos personales incluidos en el presente contrato, juntamente con los que se obtengan durante la vigencia de la relación contractual, en un fichero creado bajo la responsabilidad de <OGR> , con la finalidad de llevar a cabo la gestión de su relación. En el caso de que para la realización de los servicios contratados facilite datos personales de otras personas físicas de su organización, deberá, con carácter previo, informarles de esta cláusula. Así mismo, consiente expresamente y autoriza a <OGR>, a comunicar estos datos personales a aquellas entidades la intervención de las cuales sea prevista y/o necesaria para dar cumplimiento a esta relación contractual.

En virtud de lo que dispone el artículo 15 y siguientes de la vigente Ley 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, en cualquier momento el titular de los datos podrá ejercitar su derecho al acceso, rectificación, cancelación y oposición, dirigiéndose por escrito a la dirección de las partes indicadas en este contrato.

SEXTA. – La recisión, resolución o extinción del contrato de prestación de servicios, justificará la obligación por parte de <OGR>, de cancelar los datos de carácter personal facilitados por parte de <Universidad>. Estos datos deberán ser destruidos o retornados a <universidad> según esta determinación, al igual que cualquier soporte o documento en que conste algún dato de carácter personal objeto del tratamiento.

SÉPTIMA. – La <OGR> se compromete a cumplir las obligaciones establecidas en el presente contrato y en la normativa vigente, en relación al presente encargo de tratamiento.

OCTAVA. – El presente contrato se considera accesorio del contrato o contratos de prestación de servicios suscritos entre las partes, por lo cual su duración y extinción quedará supeditada a la vigencia del mismo.

NOVENA. – En lo previsto en este contrato, así como en la interpretación y resolución de los conflictos que pudieran surgir entre las partes como consecuencia del mismo, será aplicable la legislación española. Para la resolución de cualquier controversia que pudiera derivarse del presente

contrato, las dos partes se someterán a jurisdicción de los tribunales de la ciudad <XXXXXX> , con renuncia expresa a cualquier otro fuero que pudiera corresponderles.

Y para dejar constancia, y en prueba de conformidad por ambas partes, se firma el presente documento por duplicado ejemplar, y a un solo efecto, en el lugar y fecha arriba indicados.

Firmado	Firmado
<Nombre>	<Nombre>
<Universidad>	<OGR>

Modelo de protección de datos de OGR con empresas de servicio externo.

Por una parte, <OGR>, con NIF…….. y domicilio social …… representada por ……... con DNI ……. en calidad de …… .

Por la otra parte, <Empresa Servicios>, con NIF…….. y domicilio social …… representada por ……... con DNI ……. en calidad de …… .

Exponen

PRIMERA. – Que <OGR> a contratado con <Empresa Servicios> la prestación de servicio de <Empresa Servicios>.

SEGUNDA – Que por este motivo, cualquier información , sea cual sea su naturaleza (comercial, financiera, operacional o de otro tipo), en cualquier forma o soporte (ya sea verbal, escrita, gravada o de otro tipo), a la que en virtud del servicio prestado pudiera tener acceso <Empresa Servicios> , será considerada a todos los efectos como “información confidencial”.

TERCERA. – Que <Empresa Servicios>, se compromete a no utilizar esta información para su propio beneficio ni para facilitarla a ningún tercero, obligación que subsistirá una vez finalizada la relación contractual, así como a respetar y velar por el correcto seguimiento de las normas que regulan el acceso y el comportamiento de su personal en los edificios e instalaciones de <OGR>.

CUARTA. – Que <Empresa Servicios>, se comprometa a informar, formar y hacer firmar este conocimiento a todo su personal y , en especial, y de forma

ineludible, a todo aquel personal que trabaje o pueda trabajar en su nombre en <OGR>.

QUINTA. - Que <Empresa Servicios>, responderá delante <OGR>, por el daño derivado del incumplimiento de cualquiera de las obligaciones del presente contrato, y que <OGR>, tendrá derecho a reclamar las correspondientes indemnizaciones, además de emprender cualquier otra opción legal que le pueda corresponder.

Y para dejar constancia, y en prueba de conformidad por ambas partes, se firma el presente documento por duplicado ejemplar, y a un solo efecto, en el lugar y fecha arriba indicados.

Firmado	Firmado
<Nombre>	<Nombre>
<OGR>	<Empresa Servicios>

OBSERVATORIO UNIVERSIDAD Y DISCAPACIDAD

Este trabajo define un sistema global de gestión de información estadística relativa al alumnado con discapacidad en las universidades públicas españolas. Su propósito es el de facilitar a los investigadores de los ámbitos de discapacidad y educación superior acceder a dichos bancos de datos estadísticos para así poder establecer modelos, tendencias y planes de actuación, mejorando de este modo la igualdad de oportunidades de todo el alumnado.

Su aplicación es universal, pudiéndose instaurar en todas la universidades públicas españolas. Se trata de una solución de bajo coste, que prioriza el uso de software libre, y que permite adaptar necesidades futuras gracias a su escalabilidad.

UNIÓN EUROPEA
FONDO SOCIAL EUROPEO
El Fondo Social Europeo invierte en tu futuro

Fundación ONCE
para la Cooperación e Inclusión Social de Personas con Discapacidad

UNIVERSITAT POLITÈCNICA DE CATALUNYA
BARCELONATECH
Cátedra de Accesibilidad