UAM
UNIVERSIDAD AUTONOMA
DE MADRID

# PLIEGO DE PRESCRIPCIONES TÉCNICAS DEL SERVICIO DE DETECCIÓN DE PLAGIO EN LA UNIVERSIDAD AUTÓNOMA DE MADRID

## 1. Antecedentes

El uso intensivo de las TIC en la docencia y en el proceso de aprendizaje, con una importante utilización de contenidos digitales hacen del plagio un riesgo cada vez más acuciante para la UAM, como así se ha puesto de manifiesto en diferentes jornadas de la CRUE, siendo varias universidades las que han optado ya por incorporar sistemas de detección de plagio.

Esta demanda de servicio, fruto de la realidad que supone el uso de contenidos digitales en el ámbito docente, así como la necesidad de establecer un modelo homogéneo de detección del mismo en los diferentes ámbitos de la Universidad hacen necesario el uso de una plataforma que disponga de todos los elementos que permitan la detección del plagio en contenidos digitales utilizados y generados en la universidad. La detección del plagio es, de este modo, un instrumento que contribuye a la correcta evaluación de las destrezas y competencias de los estudiantes, manifestadas en los materiales y trabajos elaborados en forma electrónica en los distintos ámbitos de aprendizaje e investigación de la Universidad.

## 2. Objeto

### 2.1 Alcance

El objetivo de este proyecto es la contratación de un servicio que facilite el uso de una plataforma de detección de plagio en modalidad "Software As A Service" (en adelante SaaS). Esta plataforma se establecerá como pieza fundamental para detección de plagios en contenidos utilizados y generados en la UAM.

Los servicios requeridos, además de la explotación de la plataforma, deben incluir el mantenimiento correctivo y evolutivo de la propia plataforma ofertada, así como el soporte técnico de la misma.

### 2.2 Ubicación

Los servicios de mantenimiento y soporte serán prestados por personal cualificado en los entornos tecnológicos descritos en el presente pliego. La prestación de los servicios podrá realizarse de forma remota utilizando medios telefónicos o electrónicos.

### 2.3 Horario de Prestación de Servicios

La plataforma ofertada deberá estar disponible para su uso en modalidad SaaS, con una disponibilidad 24x7 los 365 días del año. Para la prestación de los servicios de mantenimiento y soporte se establece un horario entre las 09:00 y las 18:30 de lunes a viernes.

## 3. Entorno Tecnológico

Este apartado describe el entorno tecnológico que sustenta el uso de la plataforma de detección de plagio en modalidad SaaS.

### 3.1 Comunicaciones

La conectividad de la UAM con Internet está garantizada al formar parte de la red de I+D nacional, RedIRIS. Puede consultarse la estructura de la red nacional así como sus puntos de presencia en la UAM y la conectividad con redes externas en http://www.rediris.es/lared/.

La alta disponibilidad de esta red de comunicaciones, su alta capacidad y la capilaridad que se consigue a

través de su extensión en la UAM a través de la red de comunicaciones interna facilita el uso de plataformas software externas a la institución explotadas en modo remoto.

### 3.2 Plataforma de Campus Virtual

El campus virtual de la UAM está soportado principalmente por la plataforma LMS (Learning Management System) de fuentes abiertas Moodle, en su versión 3.x. Esta plataforma automatiza todos los procesos de publicación de contenidos de aprendizaje y seguimiento del mismo. Permite, entre otros, gestionar usuarios, materiales y actividades de formación, administrar el acceso, controlar el seguimiento del proceso de aprendizaje, recibir trabajos o informes elaborados por los estudiantes, realizar evaluaciones, generar informes y gestionar servicios de comunicación como foros de discusión.
Esta plataforma, integrada en La Docencia En Red de la Universidad, se establecerá como pieza fundamental para detección de plagios en contenidos utilizados y generados en la UAM.

- Sólo el profesorado podrá remitir documentos y recibir informes del servicio para la detección de plagios.
- El número de estudiantes matriculados en un curso académico asciende a 40.000.
- El envío de documentos al servicio se realizará bajo demanda. Es el profesorado quien decide qué documentos analizar y cuándo hacerlo. Como consecuencia, no todos los documentos almacenados en Moodle serán analizados.

Además, La UAM también dispone de otra plataforma tecnológica (plataforma open edX, versión Cypress), de uso más limitado, que da soporte a sus cursos SPOC (*Small Private Online Course*) de la UAM, y para la que sería también necesario contar con el sistema antiplagio que controle el seguimiento del proceso de aprendizaje de los estudiantes respecto de los trabajos presentados a través de esta plataforma.

## 4. Funcionalidades Requeridas

Este apartado expone los requisitos funcionales necesarios para la prestación del servicio de detección de plagio a través de una plataforma explotada en modalidad SaaS. Estos requisitos se exponen agrupados en bloques y enumerados de forma independiente.

### 4.1 Requisitos Generales

**Multiplataforma**
La plataforma de detección de plagio deberá permitir el uso como clientes de usuario de equipos basados en sistemas operativos Windows, MAC y Linux, accediendo con los navegadores web más habituales: Mozilla Firefox, MS Internet Explorer, Google Chrome, Safari y Opera.

**Conectividad Web**
La plataforma de detección de plagio deberá ser accesible utilizando exclusivamente conectividad web http y https con el equipo cliente del usuario.

**Clientes**
La plataforma de detección de plagio deberá permitir el uso de la misma sin necesidad de realizar un despliegue de software cliente previo al establecimiento de la comunicación.

**Manual de Usuario**
La plataforma de gestión de plagio deberá disponer de un manual de usuario que facilite su utilización a los diferentes perfiles de usuario con acceso a la misma.

UNIVERSIDAD AUTONOMA DE MADRID

**Protección de Datos de Carácter Personal**

En caso de incorporar a sus sistemas documentos que contengan datos, como el nombre y apellidos del autor de un documento o cualesquiera otros, el adjudicatario tendrá la condición de encargado del tratamiento al efecto de lo dispuesto en la legislación sobre protección de datos personales. En virtud de ello:

1.- Deberá cumplir con lo dispuesto por la Disposición adicional vigésima sexta sobre "Protección de datos de carácter personal" del Real Decreto Legislativo 3/2011, de 14 de noviembre, por el que se aprueba el texto refundido de la Ley de Contratos del Sector Público, por el artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal y por los artículos 20 y siguientes del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

2.- Deberá facilitar la tramitación y firma del contrato para el acceso a los datos por cuenta de terceros al que se refieren las normas citadas. En particular:

a) Deberá acreditar su capacidad para cumplir con sus obligaciones en esta materia de modo que se pueda realizar una elección diligente del encargado en los términos del artículo 20 del Real Decreto 1720/2007. Tales capacidades podrán demostrarse entre otras formas mediante:

- Acreditación de la inscripción de sus propios ficheros ante el registro General de Protección de Datos Personales de la Agencia Española de Protección de Datos o, en su caso, acreditación del cumplimiento de la normativa nacional que le resulte de aplicación.

- Exhibición o certificación de informes de auditoría que acrediten el cumplimiento normativo y/o de seguridad.

- Acreditación de la adhesión a estándares comúnmente admitidos en materia de seguridad o privacidad y cuando ello fuere posible exhibición de su certificación de cumplimiento. Se considerarán relevantes:

* La serie de normas ISO/IEC 27000 y específicamente la ISO/IEC 27018:2014 — Information technology — Security techniques — Code of practice for protection of Personally Identifiable Information (PII) in public clouds acting as PII processors.

* EuroCloud Star Audit Certification for Cloud Services.

* CSA Security, Trust and Assurance Registry (STAR) Program.

- Acreditación de que su personal ha sido debidamente formado o de contar con un data protection officer en su plantilla.

- Declaración de sus políticas de seguridad en aquello que pudiera afectar al objeto del contrato objeto de licitación.

b) Deberá facilitar cuando se le requiera la información necesaria para la redacción definitiva del citado contrato.

c) Deberá firmar el citado contrato necesariamente antes del desarrollo de actividades que comporten acceso a datos.

3. Cuando se trate de un entidad que realice sus los tratamientos en un Estado Miembro de la Unión Europea deberá aportar una descripción de las medidas de seguridad aplicable conforme a la legislación de dicho estado.

Si el tratamiento se realizase en España, los medios técnicos ofrecidos para la prestación del servicio deberán garantizar el cumplimiento de lo dispuesto por la Disposición adicional única sobre productos de software del Real Decreto 1720/2007 incorporando una descripción técnica del producto en sus dimensiones de hardware y software que acredite la capacidad de cumplir el nivel básico de seguridad previsto por el Título VIII.

4. Tratamientos mediante servicios de Cloud.

En caso de que la aplicación se provea en un entorno de Cloud Computing, ya se provea con medios propios o mediante una subcontratación, el adjudicatario:

a) Declarará expresamente si dichos servicios de Cloud se proveen en un país del Espacio Económico Europeo o en un país tercero.

b) En caso de que los tratamientos en Cloud se realicen en un país tercero:

- Indicará el país o la lista de países en los que se tratarán los datos.

- Indicará si tales servicios se realizan mediante subcontratación de terceros así como la identificación de tales terceros o la referencia a la página web en la que el tercero autorizado mantiene actualizada la lista de subcontratistas.

- Garantizará el cumplimiento de sus obligaciones y en particular las relativas a la regulación de las transferencias internacionales de datos personales por los artículos 33 y 34 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y el Título VI del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

A tal efecto aportará, si procede, el documento que acredite bien que la transferencia internacional de datos se realiza a un país declarado seguro por la Comisión Europea, bien haber formalizado un contrato al amparo de las llamadas Decisiones Contractuales Tipo de la Comisión para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países y contar con la debida autorización de la Autoridad Nacional de Protección de Datos conforme a la legislación interna que resulte de aplicación.

- Podrá tomarse como referencia para el cumplimiento los documentos de la AEPD "Guía para clientes que contraten servicios de Cloud Computing – 2013" y las "Orientaciones para prestadores de servicios de Cloud Computing – 2013", así como el Dictamen 5/2012 sobre la computación en la nube del Grupo de Protecciones del Artículo, 29 de la Directiva 95/46/CE.

**Cumplimiento de normativas relativas a seguridad de datos e información.**

En el desarrollo de su actividad, por error o accidente, el proveedor puede llegar a acceder a datos de carácter personal con motivo de la prestación del servicio. Por tal motivo la empresa adjudicataria deberá firmar una declaración de confidencialidad y seguridad anexa al contrato principal en los términos del artículo 83 del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

Además, en todas las actuaciones objeto del presente contrato la empresa adjudicataria se compromete a cumplir los requisitos de seguridad y confidencialidad contenidos en las siguientes normas:

Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y reglamento aprobado por el Real decreto 1720/2007 de 21 de diciembre.

Real Decreto 3/2010, de 8 de enero, por el que se reguila el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

Política de seguridad de la información en la utilización de medios electrónicos de la Universidad Autónoma de Madrid, y normativa de desarrollo.

Reglamento de seguridad de la información en la utilización de medios electrónicos de la Universidad Autónoma de Madrid.

Así como las instrucciones específicas del Comité de Seguridad y del responsable de Seguridad de la Universidad Autónoma de Madrid

**Propiedad Intelectual**

El proveedor de la plataforma de detección de plagio deberá garantizar el cumplimiento de la legislación vigente en materia de Propiedad Intelectual, debiendo indicar en su oferta las medidas de seguridad adoptadas a tal efecto.

**Proceso de Reversión de Servicio**

El proveedor de la plataforma de detección de plagio deberá indicar el procedimiento estipulado para la

reversión del servicio, tanto en el caso de la finalización de la vigencia de este contrato como en el caso de terminación temprana del servicio.

**Movilidad**

La plataforma de detección de plagio permitirá su utilización desde dispositivos móviles. El proveedor deberá indicar en su oferta las funcionalidades asociadas a estas aplicaciones.

## 4.2 Requisitos Asociados a la Administración

**Gestión de usuarios**

La plataforma de detección de plagio facilitará la gestión de diferentes perfiles y la generación de usuarios individuales asociados a estos roles según corresponda. Será necesaria la autenticación contra los servicios de autenticación de la UAM basados en el protocolo LDAP o mediante la integración con el servicio de autenticación integrado de RedIRIS (SIR4).

## 4.3 Requisitos Asociados a la Integración

**Integración Moodle**

La plataforma de detección de plagio facilitará la integración con la plataforma soporte del Campus Virtual de la Universidad, basada en Moodle v 3.x. Se deberá indicar claramente en la oferta el procedimiento de integración y las funcionalidades aportadas sobre Moodle en materia de detección del plagio, entre las que se incluirá la detección de plagio en el componente de Tareas de Moodle. Teniendo en cuenta que el análisis antiplagio se realizará a demanda del profesorado responsable de la asignatura y pudiendo realizarse de manera selectiva sobre un conjunto de documentos.

**Integración Open edX**

Se valorará positivamente que la plataforma de detección de plagio facilite la integración con la plataforma soporte del Campus Virtual de la Universidad para cursos online, basada en Open edX. Se deberá indicar claramente en la oferta el procedimiento de integración y las funcionalidades aportadas sobre Open edX en materia de detección del plagio. Teniendo en cuenta que el análisis antiplagio se realizará a demanda del profesorado responsable de la asignatura y pudiendo realizarse de manera selectiva sobre un conjunto de documentos.

## 4.4 Requisitos Asociados a los Contenidos

**Gestión de Contenidos Propios**

La plataforma de detección del plagio facilitará la diferenciación de los contenidos subidos a la plataforma por usuarios de la UAM. Será potestad de la universidad decidir si permite que estos contenidos puedan ser utilizados como fuente para la detección del plagio en otras instituciones de educación superior en el ámbito nacional e internacional.

**Proceso de Incorporación de Contenidos**

La plataforma de detección de plagio facilitará la automatización del proceso de subida de múltiples documentos. Esta incorporación deberá permitir al menos la incorporación individual de ficheros, de múltiples ficheros de forma simultánea y de múltiples ficheros comprimidos en un único fichero tipo ZIP, RAR o similar.

El servicio debe permitir el análisis de documentos en múltiples formatos, siendo fundamental que permita los formatos más habituales en aplicaciones ofimáticas: ".txt", ".pdf", ".rtf", ".doc",".docx",".odt", ".xls",".xlsx", ".ppt",".pptx"

**Informes**

La plataforma de detección de plagio facilitará la consulta de los ficheros subidos a la misma por cada uno de sus usuarios mediante informe o consulta desarrollada a tal efecto.

### 4.5 Requisitos Asociados a la Detección del Plagio

**Fuentes Externas**

La plataforma de detección de plagio deberá realizar los procesos necesarios para identificar el plagio con respecto a fuentes fidedignas existentes. Se considera necesario incluir en la oferta las diferentes fuentes o tipos de fuentes contra los que se realizará este proceso. Al menos se considera necesaria la existencia de 10 fuentes diferentes.

**Fuentes Internas a la Organización**

La plataforma de detección de plagio facilitará que el proceso de detección de plagio incluya el contenido generado por los propios usuarios de la UAM.

El servicio ofertado proporcionará, con independencia del acceso integrado con el Aula Virtual, un portal de acceso personal que permita al profesorado de la Universidad tener acceso individualizado a los documentos e informes gestionados a través de la plataforma de detección de plagios. El acceso a este portal deberá estar integrado con el directorio de usuarios de la UAM.

**Fuentes Internas a la Plataforma**

La plataforma de detección de plagio facilitará la consideración como fuente de otras instituciones de educación superior que así lo permitan para posibilitar que el proceso de detección de plagio incluya el contenido generado por ellas y albergado en la misma plataforma.

**Resultado del Proceso**

La plataforma de detección de plagio facilitará la consulta de los resultados del proceso de detección, permitiendo que el usuario decida el medio por el que ser informado que debe incluir el correo electrónico.

## 5. Servicios Requeridos

Este punto identifica los servicios solicitados para el uso de la plataforma de detección de plagio cuyos entornos tecnológicos y requisitos funcionales se han descrito anteriormente. La prestación de todos los servicios se realizará mediante los protocolos de actuación acordados con el Jefe de la Unidad Técnica de Sistemas de Gestión de la UAM. El seguimiento global del proyecto se realizará en coordinación con el Vicerrectorado de Tecnologías para la Educación de la UAM o con el Vicerrectorado que en ese momento tenga atribuidas las competencias en materia de Tecnologías de la Información.

### 5.1 Derechos de Uso

Este servicio comprende el uso de la plataforma software en modo SaaS con los módulos necesarios para satisfacer como mínimo los requisitos expuestos en el punto anterior y capacidad ilimitada para realizar detecciones de plagio a lo largo del periodo del contrato, sin limite máximo de usuarios que puedan realizar una consulta a través de la plataforma ni de archivos sometidos a revisión.

### 5.2 Actualización de Software

Este servicio comprende la puesta a disposición del software más actualizado para la plataforma de detección de plagio en uso bajo modalidad SaaS a lo largo del periodo del contrato. Estas actualizaciones deben garantizar el cumplimiento de la legislación vigente en las materias afectadas por la protección de datos y propiedad intelectual.

### 5.3 Mantenimiento Correctivo

Se incluyen en estos servicios la realización de actuaciones destinadas a resolver cualquier incidencia que afecte al entorno tecnológico descrito anteriormente.

## 6. Niveles de Servicio

### 6.1 Mantenimiento Correctivo

En función de la importancia, las incidencias trasladadas al proveedor serán clasificadas en:

- Críticas. Serán aquellas que impiden el funcionamiento básico de las aplicaciones.
- Urgentes. Serán aquellas que impiden desarrollar funciones adicionales en las aplicaciones.
- Ordinarias. Ninguna función se encuentra degradada y puede resolverse por medios alternativos.
- Leves. Aquellos con bajo nivel de importancia.

En función de los niveles de criticidad se definen los siguientes tiempos máximos de resolución:

- Críticas: 16 horas laborables (Tiempo máximo de resolución)
- Urgente: 5 días laborables (Tiempo máximo de resolución)
- Ordinaria: 14 días laborables (Tiempo máximo de resolución)
- Leve: 30 días laborables (Tiempo máximo de resolución)

Los tiempos de respuesta se contabilizan desde el momento en el que la comunicación se registra en el sistema de gestión de incidencias de la UAM. El procedimiento permitirá a la UAM proponer la criticidad de la comunicación. Toda comunicación recibida deberá ser catalogada por el adjudicatario, revisando la criticidad propuesta por la Universidad en un tiempo máximo, salvo casos absolutamente excepcionales y justificados, de 60 minutos en horario laboral.

### 6.2 Disponibilidad

Se establece la necesidad de garantizar la disponibilidad de las funcionalidades adquiridas por la UAM a través de la plataforma de detección de plagio por encima del 98%. Se entiende como disponibilidad completa (100%) el funcionamiento correcto de la aplicación software en todos sus componentes durante 24 horas al día, 7 días a la semana. El fallo o disminución estimable del rendimiento de cualquier componente achacable al sistema software durante cualquier intervalo de tiempo es una pérdida parcial de disponibilidad durante ese intervalo.

La disponibilidad se calcula, mes a mes, como el porcentaje entre el tiempo total de funcionamiento correcto y el tiempo de disponibilidad completa. No se computará como tiempo de funcionamiento incorrecto el achacable a las siguientes circunstancias, cuando éstas no vengan derivadas de un funcionamiento incorrecto de la aplicación:

- Actualización de versiones que exijan la desconexión de los usuarios a la aplicación.
- Fallo en la seguridad de la red de la UAM.
- Fallo en la seguridad de sistemas de la UAM.
- Caídas de los equipos y servicios de red de la UAM.
- Fallos en el hardware de la UAM implicado en el uso de la aplicación.

El adjudicatario informará a la Universidad, con tiempo suficiente, de los mecanismos de seguimiento y supervisión que utilizará para garantizar la disponibilidad.

### 6.3 Rendimiento

Se establece la necesidad de garantizar el funcionamiento de la aplicación en unos márgenes de rendimiento aceptables. Se entiende un rendimiento aceptable como aquél que permite el acceso y uso

simultáneo de la aplicación al número de usuarios que se ha definido durante la fase de implantación, con tiempos de respuesta considerados como aceptables en aplicaciones similares y en entornos de explotación homólogos.

Como medida mínima de rendimiento, la plataforma de detección de plagio deberá garantizar un rendimiento que suponga la finalización del proceso de detección en un tiempo inferior a las 24 horas.

El adjudicatario informará a la Universidad, con tiempo suficiente, de los mecanismos de seguimiento y supervisión que utilizará para garantizar el rendimiento, así como las métricas utilizadas para medirlo.

# 7. Responsabilidades

## 7.1 Responsabilidades de la UAM

En el marco del presente servicio, la UAM se compromete a:

- Designar a un interlocutor con la empresa para la coordinación general del servicio y un interlocutor técnico que facilitará la coordinación para cada uno de los servicios solicitados.
- Proporcionar el acceso a las infraestructuras y servicios universitarios necesarios para el desarrollo de los servicios de soporte descritos.
- Documentar los distintos protocolos de actuación que se vayan incorporando, coordinando con el adjudicatario la mejora de los mismos.
- Facilitar la documentación necesaria para la realización de los diferentes servicios de soporte, incluyendo las políticas corporativas en materia de seguridad, protección de datos y gestión de aplicaciones.
- Comunicar con antelación aquellos cambios tecnológicos o de infraestructura que puedan producirse en la UAM y afecten al servicio contratado, para que sean incorporados de forma coordinada con el adjudicatario.

## 7.2 Responsabilidad de la Empresa Adjudicataria

En lo que se refiere a términos generales en la prestación de servicios, la empresa adjudicataria debe cumplir los requisitos impuestos en el Pliego de Prescripciones Técnicas y Cláusulas Administrativas del presente concurso, incluyendo los relativos a protección de datos, confidencialidad y propiedad intelectual. En el marco del presente servicio, la empresa adjudicataria se compromete a:

- Designar a un interlocutor con la UAM para labores de coordinación global, así como interlocutores con responsabilidad sobre la prestación de cada uno de los servicios descritos.
- Usar los recursos que la UAM pone a su disposición con los fines exclusivos que se expresan en este documento.
- Comunicar con antelación aquellos cambios tecnológicos o de infraestructura que puedan producirse en el adjudicatario y afecten al servicio contratado, para que sean incorporados de forma coordinada con la UAM.

# 8. Variantes y Mejoras

No se admiten variantes. Se admitirán mejoras conforme a lo establecido en el pliego de cláusulas administrativas particulares.

UNIVERSIDAD AUTONOMA DE MADRID

# 9. Alcance del Servicio

## 9.1 Periodo de Prestación de los Servicios

Se establece un periodo de prestación de los servicios descritos de **36 meses**, desde el 1 de octubre de 2016 al 30 de septiembre de 2019.

## 9.2 Lugar de Prestación de los Servicios

La prestación de los servicios se podrá realizar de forma remota mediante medios electrónicos.

## 9.3 Alcance Económico

Se estima un alcance máximo para la totalidad del período de tiempo objeto el presente proyecto (36 meses) de **72.600**€ IVA incluído.

## 9.4 Facturación

La facturación del presente servicio se realizará a través de pagos mensuales.

Madrid, 15 de julio de 2016.
La Directora de Tecnologías de la Información,

María José García Rodríguez.

**Esta Gerencia, por delegación del Sr. Rector de esta Universidad, de fecha 10 de abril de 2015 (BOCM de 17-04-2015) ha resuelto aprobar el presente Pliego de Prescripciones Técnicas.**

**Madrid, 26 de julio de 2016**
**EL GERENTE**

UNIVERSIDAD AUTÓNOMA DE MADRID GERENCIA

**Teodoro Conde Minaya**