



**Resolución Rectoral de 22 de febrero de 2011, por la que se hace pública la Política de Seguridad de la Información de la Universidad Pablo de Olavide, de Sevilla, aprobada por el Consejo de Dirección en su sesión del 8 de febrero de 2011**

Ante la necesidad de definir una política de seguridad de la información, en la que se establezcan directrices básicas y duraderas para una protección eficaz de los sistemas gestionados por la Universidad y de la información almacenada en los mismos, el Consejo de Dirección, de conformidad con lo previsto en el artículo 31.2 de los Estatutos de la Universidad Pablo de Olavide, de Sevilla, aprobados por Decreto 298/2003, de 21 de octubre (BOJA de 6 de noviembre de 2003, corrección de errores BOJA de 1 de diciembre de 2003 y BOE de 23 de diciembre de 2003), aprobó, en sesión de 8 de febrero de 2011, la Política de Seguridad de la Información de la Universidad Pablo de Olavide, de Sevilla, previo informe de la Comisión de Seguridad de Tecnologías de la Información, creada por acuerdo del Consejo de Gobierno de la Universidad de 28 de junio de 2010.

Este Rectorado, en uso de las atribuciones que legalmente tiene conferidas, RESUELVE:

ÚNICO.-. Hacer pública la Política de Seguridad de la Información de la Universidad Pablo de Olavide, de Sevilla, aprobada por el Consejo de Dirección en su sesión del 8 de febrero de 2011

En Sevilla, a 22 de febrero de 2011

Fdo.: EL RECTOR  
Juan Jiménez Martínez



Carretera de Utrera, Km.1 – 41013 Sevilla – España

Código Seguro de verificación: +039FY5Q9vvfpZdG7qYEUjJLYdAU3n8j. Permite la verificación de la integridad de una copia de este documento electrónico en la dirección: <https://portafirmas.upo.es/verificarfirma/>  
Este documento incorpora firma electrónica reconocida de acuerdo a la Ley 59/2003, de 19 de diciembre, de firma electrónica.

FIRMADO POR	JIMENEZ MARTINEZ JUAN		FECHA	25/02/2011
ID. FIRMA	juno.upo.es	+039FY5Q9vvfpZdG7qYEUjJLYdAU3n8j	PÁGINA	1 / 8
 +039FY5Q9vvfpZdG7qYEUjJLYdAU3n8j				



## POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE LA UNIVERSIDAD PABLO DE OLAVIDE, DE SEVILLA. APROBADA POR EL CONSEJO DE DIRECCIÓN EN SU SESIÓN DEL 8 DE FEBRERO DE 2011

### 1. Introducción.

El ingente volumen de información generado en la Universidad Pablo de Olavide, de Sevilla, motiva que se gestione una gran cantidad de datos en los sistemas de información de la misma. Este hecho, y el uso extensivo de tecnologías de la información en la Universidad, hace necesario definir una política de seguridad de la información, con el objetivo de establecer directrices básicas y duraderas para una protección eficaz de los sistemas gestionados por la Universidad y de la información almacenada en los mismos.

La presente política de seguridad de la información es el marco de referencia para establecer el Sistema de Gestión de la Seguridad de la Información (SGSI) de la Universidad Pablo de Olavide.

El enfoque para la gestión de la seguridad adoptado en el SGSI se basa en el recomendado por la norma UNE-ISO/IEC 27001 («Sistemas de Gestión de la Seguridad - Requisitos»).

Las directrices recogidas en este documento han sido elegidas de acuerdo con el estándar UNE-ISO/IEC 27002 («Código de buenas prácticas para la Gestión de la Seguridad de la Información»), que establece un marco de referencia de seguridad respaldado y reconocido internacionalmente.

Este marco tecnológico, organizativo y procedimental de seguridad se soporta en un conjunto de normas, estándares, procedimientos y herramientas de seguridad para la protección de la información, entre ellos la metodología MAGERIT de análisis y gestión de riesgos.

La aprobación de esta política manifiesta el interés de Universidad Pablo de Olavide en la gestión de la seguridad de la información y en la mejora continua del SGSI. Con ella se establecen los objetivos y las responsabilidades necesarias para proteger los activos de información (informaciones de interés para la Universidad, junto con los medios que se usen para procesarlas), garantizando la integridad, disponibilidad y confidencialidad de los mismos, cumpliendo con el marco legal vigente y respetando las directrices, normas y procedimientos que oportunamente se establezcan.

La Universidad Pablo de Olavide establecerá las medidas técnicas, organizativas y de control que garanticen la consecución de estos objetivos.

Carretera de Utrera, Km.1 – 41013 Sevilla – España

Código Seguro de verificación: +039FY5Q9vvfpZdG7qYEUjJLYdAU3n8j. Permite la verificación de la integridad de una copia de este documento electrónico en la dirección: <https://portafirmas.upo.es/verificarfirma/>. Este documento incorpora firma electrónica reconocida de acuerdo a la Ley 59/2003, de 19 de diciembre, de firma electrónica.

FIRMADO POR	JIMENEZ MARTINEZ JUAN		FECHA	25/02/2011
ID. FIRMA	juno.upo.es	+039FY5Q9vvfpZdG7qYEUjJLYdAU3n8j	PÁGINA	2 / 8
 +039FY5Q9vvfpZdG7qYEUjJLYdAU3n8j				



## 2. Ámbito de aplicación.

El alcance de la política de seguridad incluye todos los Centros, Departamentos, áreas y unidades administrativas, órganos, entidades creadas o participadas mayoritariamente por la Universidad, Personal de Administración de Servicios (PAS), Personal Docente e Investigación (PDI) y estudiantes que acceden a los sistemas de información de la Universidad Pablo de Olavide, así como organismos o empresas y profesionales colaboradores.

La política de seguridad es aplicable a todos los sistemas de información de la Universidad Pablo de Olavide y/o que den soporte a sus procesos y afecta a todos los activos de información sustentados en ellos.

La política de seguridad se encuentra enmarcada en el sistema de gestión de la seguridad de la información (SGSI) de la Universidad Pablo de Olavide establecido desde el Vicerrectorado de Tecnologías de la Información y la Comunicación.

## 3. Normativa de seguridad.

El sistema de gestión de la seguridad de la información (SGSI) queda formalmente establecido mediante una normativa de seguridad, formada por la presente política y las normas, estándares y procedimientos operativos que la desarrollan.

La Comisión de Seguridad de Tecnologías de la Información se encarga de la gestión de los documentos de la normativa de seguridad, debiendo asegurar que ésta sea completa y proporcione información suficiente para definir las necesidades de protección de la información y los activos asociados a la misma en el ámbito de la Universidad Pablo de Olavide.

Los documentos de la normativa de seguridad serán publicados y divulgados con el objetivo de que sean conocidos y aplicados por todos los usuarios afectados.

## 4. Organización y gestión de la seguridad.

### 4.1. Responsabilidad general.

Todos y cada uno de los usuarios de los sistemas de información de la Universidad Pablo de Olavide son responsables de la seguridad de los activos de información mediante un uso correcto de los mismos, siempre de acuerdo con sus atribuciones profesionales y académicas.

Carretera de Utrera, Km.1 – 41013 Sevilla – España

Código Seguro de verificación: +039FY5Q9vvfpZdG7qYEUjJLYdAU3n8j. Permite la verificación de la integridad de una copia de este documento electrónico en la dirección: <https://portafirmas.upo.es/verificarfirma/>. Este documento incorpora firma electrónica reconocida de acuerdo a la Ley 59/2003, de 19 de diciembre, de firma electrónica.

FIRMADO POR	JIMENEZ MARTINEZ JUAN		FECHA	25/02/2011
ID. FIRMA	juno.upo.es	+039FY5Q9vvfpZdG7qYEUjJLYdAU3n8j	PÁGINA	3 / 8
 +039FY5Q9vvfpZdG7qYEUjJLYdAU3n8j				



#### 4.2. Responsabilidad específica.

La gestión de los procesos de seguridad recogidos en el SGSI de la Universidad Pablo de Olavide es responsabilidad de un conjunto de personas con funciones concretas, definidas y documentadas.

El personal que desempeñe tareas específicas relacionadas con seguridad de la información recibirá la formación adecuada que se ajuste a sus funciones y nivel de responsabilidad.

Para una mejor respuesta ante incidentes de seguridad, la Universidad Pablo de Olavide mantendrá relaciones de cooperación en materia de seguridad con las autoridades competentes, proveedores de servicios informáticos o de comunicación, así como organismos públicos o privados dedicados a promover la seguridad de los sistemas de información.

#### 4.3. Criterios de estimación de riesgos

El análisis y gestión de los riesgos será parte esencial del proceso de seguridad de la información. Está gestión debe orientarse a mantener los riesgos en niveles aceptables, proporcionando el análisis una base de referencia para la aplicación de medidas, que serán en todo caso equilibradas y proporcionales a la naturaleza de los datos, su tratamiento y su exposición. Para el análisis y gestión de los riesgos, sin perjuicio de lo establecido por las leyes aplicables, se empleará alguna metodología reconocida internacionalmente.

#### 5. Clasificación y Control de Activos.

Los recursos informáticos y la información de la Universidad Pablo de Olavide se encontrarán inventariados, con un responsable asociado y, en caso de ser necesario, un custodio de los mismos. Los inventarios se mantendrán actualizados para asegurar su validez.

Los activos de información estarán clasificados de acuerdo a su sensibilidad y criticidad para el desarrollo de la actividad de la Universidad, en función de la cual se establecerán las medidas de seguridad exigidas para su protección.

#### 6. Seguridad física y ambiental.

Los sistemas de información serán emplazados en áreas seguras protegidas con controles de acceso físicos adecuados al nivel de criticidad de los mismos. Los sistemas y la información que soportan estarán adecuadamente protegidos frente a amenazas físicas o ambientales, sean éstas intencionadas o accidentales.

Carretera de Utrera, Km.1 – 41013 Sevilla – España

Código Seguro de verificación: +039FY5Q9vvfpZdG7qYEUjJLYdAU3n8j. Permite la verificación de la integridad de una copia de este documento electrónico en la dirección: <https://portafirmas.upo.es/verificarfirma/>  
Este documento incorpora firma electrónica reconocida de acuerdo a la Ley 59/2003, de 19 de diciembre, de firma electrónica.

FIRMADO POR	JIMENEZ MARTINEZ JUAN		FECHA	25/02/2011
ID. FIRMA	juno.upo.es	+039FY5Q9vvfpZdG7qYEUjJLYdAU3n8j	PÁGINA	4 / 8
 +039FY5Q9vvfpZdG7qYEUjJLYdAU3n8j				



## 7. Gestión de sistemas, operaciones y comunicaciones.

La Universidad Pablo de Olavide asegurará la correcta gestión y operación de los sistemas de información estableciendo estándares de seguridad y adoptando las mejores prácticas en materia de seguridad (configuración, mecanismos de protección, actualización, monitorización, detección de vulnerabilidades, respaldo de información, etc.).

Las incidencias relacionadas con seguridad de la información serán registradas, notificadas y resueltas a la mayor brevedad posible por el personal asignado para ello.

## 8. Control de acceso.

La Universidad Pablo de Olavide pone a disposición de sus usuarios la capacidad de acceder a sus sistemas de información y visualizar o modificar la información que procesan y almacenan.

Los permisos de acceso a las redes, sistemas y a la propia información serán otorgados mediante un proceso formal de aprobación que asegure que los usuarios tengan acceso únicamente a los recursos e información necesarios para el desempeño de sus funciones en la Universidad.

Todos los empleados y personal externo, así como entidades colaboradoras que accedan a los sistemas de información de la Universidad Pablo de Olavide, quedarán registrados y dispondrán de credenciales personales e intransferibles. Toda persona registrada que disponga de credenciales de acceso será responsable de mantener su confidencialidad y asegurar su correcto uso.

## 9. Desarrollo y mantenimiento de sistemas.

Las aplicaciones que se desarrollen para la Universidad Pablo de Olavide deberán contemplar aspectos de seguridad de la información en todas las fases del ciclo de vida de desarrollo, desde la toma de requisitos hasta la realización de pruebas y el paso a producción.

## 10. Gestión de continuidad de actividad.

La Universidad Pablo de Olavide dispone de un plan para mantener la continuidad de los procesos, servicios y sistemas críticos y garantizar su recuperación en caso de desastre. La finalidad de este plan es reducir el tiempo de indisponibilidad a niveles aceptables mediante la combinación de controles de carácter organizativo, tecnológico y procedimental tanto preventivos como de recuperación.

Carretera de Utrera, Km.1 – 41013 Sevilla – España

Código Seguro de verificación: +039FY5Q9vvfpZdG7qYEUjJLYdAU3n8j. Permite la verificación de la integridad de una copia de este documento electrónico en la dirección: <https://portafirmas.upo.es/verificarfirma/>. Este documento incorpora firma electrónica reconocida de acuerdo a la Ley 59/2003, de 19 de diciembre, de firma electrónica.

FIRMADO POR	JIMENEZ MARTINEZ JUAN		FECHA	25/02/2011
ID. FIRMA	juno.upo.es	+039FY5Q9vvfpZdG7qYEUjJLYdAU3n8j	PÁGINA	5 / 8
 +039FY5Q9vvfpZdG7qYEUjJLYdAU3n8j				



## 11. Conformidad.

La Universidad Pablo de Olavide adoptará las medidas técnicas y organizativas necesarias para mantener sus sistemas de información adaptados a la normativa legal vigente, y especialmente a aquellas regulaciones legales relativas al tratamiento de los datos de carácter personal, cuyas medidas específicas de tratamiento figurarán en el correspondiente Documento de Seguridad.

Es responsabilidad de todas las áreas conocer y cumplir la legislación vigente de aplicación en sus ámbitos de actuación, incluyendo especialmente las áreas responsables de desarrollo de servicios y sistemas de información.

Las contrataciones y acuerdos de nivel de servicios que se establezcan con terceros incluirán cláusulas y garantías de cumplimiento de los requisitos de seguridad que exija la Universidad Pablo de Olavide y la normativa legal vigente.

Con carácter periódico se realizarán auditorías que comprueben el grado de conformidad con la política y la legislación, y revisiones que determinen el grado de cumplimiento de los objetivos de seguridad establecidos y la eficacia de los controles establecidos. Los resultados obtenidos determinarán las líneas de actuación a seguir y las posibles acciones de mejora, preventivas y correctivas, a realizar sobre los controles y la normativa de seguridad.

Carretera de Utrera, Km.1 – 41013 Sevilla – España

Código Seguro de verificación: +039FY5Q9vvfpZdG7qYEUjJLYdAU3n8j. Permite la verificación de la integridad de una copia de este documento electrónico en la dirección: <https://portafirmas.upo.es/verificarfirma/>  
Este documento incorpora firma electrónica reconocida de acuerdo a la Ley 59/2003, de 19 de diciembre, de firma electrónica.

FIRMADO POR	JIMENEZ MARTINEZ JUAN		FECHA	25/02/2011
ID. FIRMA	juno.upo.es	+039FY5Q9vvfpZdG7qYEUjJLYdAU3n8j	PÁGINA	6 / 8
 +039FY5Q9vvfpZdG7qYEUjJLYdAU3n8j				



## ANEXO I

### Glosario

**Activo.** Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos.

**Autenticación.** Procedimiento de comprobación de la identidad de un usuario como medida de seguridad frente a posibles operaciones fraudulentas a través de la Red. La finalidad que persigue esta medida de seguridad es servir de salvaguarda para comprobar que los usuarios con los que se está interactuando son realmente quienes dicen ser. Este proceso constituye una funcionalidad característica para una comunicación segura en la Red.

**Confidencialidad.** Propiedad o atributo consistente en proporcionar acceso a los sistemas de información únicamente a aquellos usuarios autorizados, en tiempo y forma determinados, y negar el acceso a terceros no autorizados.

**Disponibilidad.** Se trata de la capacidad de un servicio, de unos datos o de un sistema, a ser accesible y utilizable por los usuarios (o procesos) autorizados cuando estos lo requieran.

**Documento de seguridad.** Se trata de un documento elaborado por el responsable del fichero o tratamiento en el que se recogen las medidas de índole técnica y organizativa acordes a la normativa de seguridad vigente que será de obligado cumplimiento para el personal con acceso a los sistemas de información.

**Integridad.** Conjunto de medidas de seguridad que se incluyen en un sistema de información, que garantizan la exactitud de los datos transportados o almacenados, evitando su alteración, pérdida o destrucción, ya sea de forma accidental, por fallos de software o hardware, por condiciones medioambientales o bien, por intervención de terceros con fines fraudulentos.

**Manual de seguridad:** Se trata del documento que inspira y dirige todo el sistema, el que expone y determina las intenciones, alcance, objetivos, responsabilidades, políticas y directrices principales, etc., del Sistema de Gestión de Seguridad de la Información (SGSI). Incluye la política que se define como Política de seguridad.

**Medidas de seguridad.** Conjunto de disposiciones encaminadas a protegerse de los riesgos posibles sobre el sistema de información, con el fin de asegurar sus objetivos de seguridad. Puede tratarse de medidas de prevención, de disuasión, de protección, de detección y reacción, o de recuperación.

**Política de seguridad.** Conjunto de directrices plasmadas en documento escrito, que rigen la forma en que una organización gestiona y protege la información y los servicios que considera críticos.

Carretera de Utrera, Km.1 – 41013 Sevilla – España

Código Seguro de verificación: +039FY5Q9vvfpZdG7qYEUjJLYdAU3n8j. Permite la verificación de la integridad de una copia de este documento electrónico en la dirección: <https://portafirmas.upo.es/verificarfirma/>  
Este documento incorpora firma electrónica reconocida de acuerdo a la Ley 59/2003, de 19 de diciembre, de firma electrónica.


FIRMADO POR	JIMENEZ MARTINEZ JUAN		FECHA	25/02/2011
ID. FIRMA	juno.upo.es	+039FY5Q9vvfpZdG7qYEUjJLYdAU3n8j	PÁGINA	7 / 8
 +039FY5Q9vvfpZdG7qYEUjJLYdAU3n8j				



**Sistema de gestión de la seguridad de la información (SGSI).** Sistema de gestión que, basado en el estudio de los riesgos, se establece para crear, implementar, hacer funcionar, supervisar, revisar, mantener y mejorar la seguridad de la información. El sistema de gestión incluye la estructura organizativa, las políticas, las actividades de planificación, las responsabilidades, las prácticas, los procedimientos, los procesos y los recursos.

Carretera de Utrera, Km.1 – 41013 Sevilla – España

Código Seguro de verificación: +039FY5Q9vvfpZdG7qYEUjJLYdAU3n8j. Permite la verificación de la integridad de una copia de este documento electrónico en la dirección: <https://portafirmas.upo.es/verificarfirma/>  
Este documento incorpora firma electrónica reconocida de acuerdo a la Ley 59/2003, de 19 de diciembre, de firma electrónica.

FIRMADO POR	JIMENEZ MARTINEZ JUAN		FECHA	25/02/2011
ID. FIRMA	juno.upo.es	+039FY5Q9vvfpZdG7qYEUjJLYdAU3n8j	PÁGINA	8 / 8
 +039FY5Q9vvfpZdG7qYEUjJLYdAU3n8j				