Fecha de publicación: 04/10/2019

BUPO N.º: 4/2019

RESOLUCIÓN de 1 de octubre de 2019 de la Universidad Pablo de Olavide, de Sevilla, por la que se aprueba la Política de Seguridad de la Información y Protección de Datos de la Universidad Pablo de Olavide, de Sevilla.

La Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas recoge, en su artículo 13, dedicado a los derechos de las personas en sus relaciones con las Administraciones Públicas, el relativo a la protección de datos de carácter personal y, en particular, a la seguridad y confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones de las Administraciones Públicas.

La Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público establece que las Administraciones Públicas se relacionarán entre sí y con sus órganos, organismos públicos y entidades vinculados o dependientes a través de medios electrónicos. Dichos medios deben asegurar la interoperabilidad y seguridad de los sistemas y soluciones adoptadas, garantizarán la protección de los datos de carácter personal y facilitarán preferentemente la prestación conjunta de servicios a los interesados. En este sentido, el artículo 156 de la citada Ley 40/2015, de 1 de octubre, regula el Esquema Nacional de Seguridad (en adelante, ENS).

El Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, modificado parcialmente por el Real Decreto 951/2015, de 23 de octubre, establece los principios básicos y los requisitos mínimos que permitan una protección adecuada de la información y tiene por objeto determinar la política de seguridad en la utilización de medios electrónicos en su ámbito de aplicación.

El artículo 11 del citado Real Decreto 3/2010, de 8 de enero, exige que todos los órganos superiores de las Administraciones publicas dispongan formalmente de su política de seguridad, que se aprobará por el titular del órgano superior correspondiente. Esta política de seguridad se establecerá con base en los principios básicos recogidos en el capítulo II de la citada norma (seguridad integral, gestión de riesgos, prevención, reacción y recuperación, líneas de defensa, reevaluación periódica, y función diferenciada) y desarrollará una serie de requisitos mínimos consignados en el ya mencionado artículo 11, en su apartado primero.

Para dar cumplimiento a estas disposiciones, tanto las contenidas en el ENS como las exigibles en las relaciones electrónicas en el ámbito del sector público, inicialmente recogidas en la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos, la Universidad Pablo de Olavide aprobó, mediante resolución rectoral de 11 de julio de 2013, su Política de Seguridad de la Información, vigente hasta la fecha (que sustituyó a la previamente aprobada el 8 de febrero de 2011).

El órgano competente para proponer y revisar dicha Política de Seguridad, la Comisión de Seguridad de la Información, integró entre sus funciones las de supervisar y velar por el cumplimiento de las obligaciones en materia de implantación, coordinación y control de las medidas de seguridad aplicables al tratamiento de carácter personal tratados en los sistemas de información de la Universidad, de forma automatizada o no automatizada, en los términos expuestos en el Documento de Seguridad aprobado mediante resolución rectoral de 11 de julio de 2013.

BUPO N.º: 4/2019 Fecha de publicación: 04/10/2019

Una de las razones para integrar dichas funciones en la citada comisión fue el que entre sus miembros se encontrasen, entre otros, los titulares del vicerrectorado competente en Tecnologías de la Información y la Comunicación y de la Secretaría General de la Universidad, a los efectos de garantizar no sólo la correcta implantación de los procedimientos técnicos sino también la de aquéllos que afectan a las garantías legales en el tratamiento de datos personales, conforme a la normativa vigente en esta materia.

A la vista de esta integración de funciones, la comisión pasó a denominarse Comisión de Seguridad de la Información y Protección de Datos.

La plena aplicación del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos -en adelante RGPD-), a partir del 25 de mayo de 2018, exige la adopción de medidas técnicas y organizativas apropiadas con el fin de garantizar el cumplimiento de los requisitos establecidos en el mismo, al objeto de proteger los derechos y libertades de las personas físicas con respecto al tratamiento de sus datos personales.

De este modo, el RGPD establece, en su artículo 24, dentro de las obligaciones generales del responsable del tratamiento de datos personales, que, teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el citado reglamento. Asimismo, dispone que dichas medidas se revisarán y actualizarán cuando sea necesario y que, cuando sean proporcionadas en relación con las actividades de tratamiento, entre dichas medidas se incluirá la aplicación por parte del responsable del tratamiento, de las oportunas políticas de protección de datos.

En el mismo sentido, el artículo 28 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD), referido a las obligaciones generales del responsable y encargado del tratamiento, establece que dichos responsables y encargados, teniendo en cuenta los elementos enumerados en los artículos 24 y 25 del RGPD, determinarán las medidas técnicas y organizativas apropiadas que deben aplicar a fin de garantizar y acreditar que el tratamiento es conforme con el citado reglamento, con la LOPDGDD, sus normas de desarrollo y la legislación sectorial aplicable.

A fin de poder demostrar la conformidad con el RGPD, así como con la LOPDGDD, la Universidad Pablo de Olavide, como responsable de tratamientos de datos de carácter personal, opta por adoptar una política conjunta de seguridad de la información y protección de datos, que permita recoger y delimitar con claridad las responsabilidades y funciones en ambos ámbitos, de forma que se aborden tanto las cuestiones comunes a ambos como aquellas que resultan propias de cada uno de ellos.

Esta Política define el marco de referencia que permite la gestión de la seguridad de la información y la protección de datos en el contexto de los sistemas de información y de las actividades de tratamiento con datos personales de la Universidad. En este marco general, donde, como se ha señalado, se recogen responsabilidades y funciones, se delimitan también los roles necesarios para definirla, implantarla y gestionarla. Estos roles se integran en la estructura orgánica existente, a la que la Política alcanza por completo, puesto que la seguridad de la información y la protección de datos de carácter personal deben contar con el compromiso y apoyo de todos los niveles de la organización, en particular los niveles directivos, de forma que pueda estar coordinada e integrada con el resto de iniciativas universitarias, para conformar un todo coherente y eficaz.

Consecuentemente, la Comisión de Seguridad de la Información y Protección de Datos ha procedido, en el contexto de la revisión anual de la Política de Seguridad de la Información, a modificar la misma para la incorporación de la Política de Protección de Datos de la Universidad y a elevarla a este Rectorado para su aprobación, en sustitución de la política vigente, y para su difusión a toda la comunidad universitaria.

En razón de lo expuesto, haciendo uso de las competencias que le atribuye la legislación vigente, este RECTORADO de mi cargo HA RESUELTO,

PRIMERO.- Aprobar la Política de Seguridad de la Información y Protección de Datos de la Universidad Pablo de Olavide, de Sevilla, que se incorpora como anexo en la presente resolución.

SEGUNDO.- Ordenar la publicación de esta resolución en el Boletín Oficial de la Universidad Pablo de Olavide, y la entrada en vigor de la misma a partir del día siguiente a su publicación en el mismo, quedando derogada la Resolución Rectoral de 11 de julio de 2013, de la Universidad Pablo de Olavide, de Sevilla, por la que se aprueba, y se hace pública, la Política de Seguridad de la Información.

TERCERO.- Determinar la vigencia del Documento de Seguridad, aprobado mediante resolución rectoral de fecha 11 de julio de 2013, solo en las partes del mismo que no contradigan la normativa vigente en materia de protección de datos de carácter personal y, en particular, en relación con la seguridad de dichos datos, mientras se aprueban las normas y procedimientos que desarrollen la nueva Política de Seguridad de la Información y Protección de Datos de la Universidad Pablo de Olavide.

Contra la presente resolución, que pone fin a la vía administrativa, cabe interponer, en el plazo de dos meses a contar desde el día siguiente al de su notificación o publicación, recurso contencioso-administrativo ante el Juzgado de lo Contencioso-Administrativo de Sevilla, de conformidad con el artículo 8.3 de la Ley 29/1998, de 3 de julio, reguladora de la Jurisdicción Contencioso-Administrativa (B.O.E. de 14 de julio), sin perjuicio de que potestativamente se pueda presentar recurso de reposición contra esta resolución, en el plazo de un mes, ante el mismo órgano que la dicta, en cuyo caso no cabrá interponer el recurso contencioso-administrativo anteriormente citado en tanto recaiga resolución expresa o presunta del recurso de reposición, de acuerdo con lo dispuesto en los artículo 123 y siguiente de la ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

EL RECTOR

Fdo.: Vicente Carlos Guzmán Fluja

Fecha de publicación: 04/10/2019

BUPO N.º: 4/2019

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y PROTECCIÓN DE DATOS DE LA UNIVERSIDAD PABLO DE OLAVIDE, DE SEVILLA

Anexo

Fecha de publicación: 04/10/2019

BUPO N.º: 4/2019

BUPO N.º: 4/2019 Fecha de publicación: 04/10/2019

Introducción

La Universidad Pablo de Olavide, de Sevilla, depende de los sistemas de Tecnologías de Información y Comunicaciones (TIC) para alcanzar sus objetivos. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad o confidencialidad de la información tratada o los servicios prestados.

El objetivo de la seguridad de la información es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando proactivamente a los incidentes.

La Universidad necesita para alcanzar sus objetivos el tratamiento de información que contiene datos de carácter personal y ello exige la adopción de medidas técnicas y organizativas apropiadas con el fin de garantizar el cumplimiento de los requisitos establecidos por la normativa vigente en materia de protección de datos personales. A fin de poder demostrar la conformidad con dicha normativa, la Universidad debe adoptar una política de protección de datos.

La Universidad opta por adoptar una política conjunta de seguridad de la información y protección de datos que permita recoger y delimitar con claridad las responsabilidades y funciones en ambos ámbitos, de forma que se aborden tanto las cuestiones comunes a ambos como aquellas que resultan propias de cada uno de ellos.

La aprobación de esta Política manifiesta el interés de la Universidad Pablo de Olavide en la gestión de la seguridad de la información, la protección de datos y en la mejora continua. Con ella se establecen los objetivos y las responsabilidades necesarias para proteger los activos de información y servicios garantizando la integridad, disponibilidad y confidencialidad de los mismos. De la misma manera, se establecen los objetivos y responsabilidades necesarias para garantizar la conformidad de los tratamientos de datos de carácter personal. En todo caso, los objetivos y responsabilidades se establecerán en cumplimiento 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 y deberá estar preparada para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo al artículo 7 del ENS.

Alcance

Esta Política se aplica a todos los sistemas de información y a sus activos esenciales (servicios e información) y en particular a todas las actividades de tratamiento de datos de carácter personal de los que sea responsable la Universidad Pablo de Olavide.

El alcance incluye a todos los Centros, Departamentos, Áreas y Unidades Administrativas, órganos, entidades creadas o participadas mayoritariamente por la Universidad, Personal de Administración y Servicios, Personal Docente e Investigador y estudiantes que acceden a los sistemas de información y tratan datos de carácter personal de los que sea responsable la Universidad Pablo de Olavide, así como a organismos o empresas y profesionales colaboradores, siendo de obligado cumplimiento para todos ellos, con independencia de su puesto de trabajo, condición laboral o relación por la que se accede a la información.

La Política afectará a la información y datos de carácter personal tratados por medios electrónicos y en soporte papel que la Universidad gestiona en el ámbito de sus competencias.

Misión de la Universidad Pablo Olavide, de Sevilla

Creada por la Ley andaluza 3/1997, de 1 de julio, la Universidad Pablo de Olavide, de Sevilla, nace con el objetivo prioritario de facilitar el ejercicio del derecho a la educación consagrado por el artículo 27.1 de la Constitución española de 1978.

El artículo 3 de los Estatutos de la Universidad establecen su misión, en los siguientes términos:

"Como espacio educativo de formación superior, la Universidad Pablo de Olavide está al servicio de la sociedad y se define como un lugar de reflexión y pensamiento crítico comprometido con la contribución al progreso, con la enseñanza del respeto a los derechos fundamentales y libertades públicas, con el fomento de la igualdad entre mujeres y hombres, la solidaridad y los valores humanos y con la respuesta a las necesidades y problemas de la sociedad contemporánea. La Universidad procurará la más amplia proyección social de sus actividades, estableciendo al efecto cauces de colaboración y asistencia a la sociedad para contribuir y apoyar el progreso social, económico y cultural. Igualmente, fomentará y propiciará la participación de los miembros de su comunidad universitaria en actividades y proyectos de cooperación internacional y solidaridad, así como la realización de actividades e iniciativas que contribuyan al impulso de la igualdad entre hombres y mujeres, el apoyo permanente a las personas con necesidades especiales, la cultura de la paz, el desarrollo sostenible y el respeto al medio ambiente".

Marco Normativo

La Universidad Pablo de Olavide desarrolla sus funciones en el marco normativo de la administración, de la seguridad de la información y de la protección de datos que se detalla a continuación.

La Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, tiene por objeto regular los requisitos de validez y eficacia de los actos administrativos, el procedimiento administrativo común a todas las Administraciones Públicas, incluyendo el sancionador y el de reclamación de responsabilidad de las Administraciones Públicas, así como los principios a los que se ha de ajustar el ejercicio de la iniciativa legislativa y la potestad reglamentaria. En esta Ley se fijan los derechos y obligaciones de relacionarse electrónicamente con la Administración Pública.

La Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, establece y regula las bases del régimen jurídico de las Administraciones Públicas, los principios del sistema de responsabilidad de las Administraciones Públicas y de la potestad sancionadora, así como la organización y funcionamiento de la Administración General del Estado y de su sector público institucional para el desarrollo de sus actividades. Se definen en esta Ley cómo debe llevarse a cabo la relación electrónica entre administraciones.

La Comunidad autónoma de Andalucía cuenta con una Ley propia de Administración, la Ley 9/2007, de 22 de octubre, que regula la utilización de las nuevas tecnologías, y de entre sus aportaciones hay que destacar el refuerzo de los derechos de la ciudadanía ante la gestión administrativa y su derecho a la tramitación electrónica.

Estas Leyes obligan a un profundo cambio en las Administraciones Públicas, incluidas las Universidades, y a ellas hay que unir otras normas de relevancia como el Reglamento UE 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos - RGPD), la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (modificado por el Real Decreto 951/2015 de 23 de octubre) o el Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica, además de otras disposiciones concordantes y de desarrollo de todas las mencionadas anteriormente.

Entre otras normas de referencia, también debemos incluir:

- La Ley 19/2013, de 9 de diciembre, de Transparencia, Acceso a la Información Pública y Buen Gobierno.
- La Ley 1/2014, de 24 de junio, de Transparencia Pública de Andalucía.
- La Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público.
- La Ley 59/2003, de 19 de diciembre, de Firma Electrónica.
- El Real Decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición del documento nacional de identidad y sus certificados de firma electrónica
- la Ley 7/2011, de 3 noviembre, de Documentos, Archivos y Patrimonio Documental de Andalucía.

En cuanto al marco general del régimen jurídico de la Universidad Pablo de Olavide (normativa estatal, autonómica y la aprobada por la propia Universidad), las principales normas que lo configuran se encuentran publicadas en su página web www.upo.es, en el apartado Conoce la UPO, Normativa Universitaria. Entre ellas se ha de destacar la Ley Orgánica 4/2007, de 12 de abril, por la que se modifica la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades, y el Decreto 265/2011, de 2 de agosto, por el que se aprueba la modificación de los Estatutos de la Universidad Pablo de Olavide, de Sevilla, aprobados por Decreto 298/2003, de 21 de octubre.

Con respecto al marco normativo de la Administración Electrónica, en la sede electrónica de la Universidad, dentro del apartado Normativa Reguladora, consultable en el siguiente enlace https://upo.gob.es/normativa-y-legislacion, se encuentra accesible la normativa (externa e interna) de aplicación en el ámbito de la Administración Electrónica de la Universidad Pablo de Olavide.

Principios de Seguridad de la Información y Protección de Datos

La Universidad Pablo de Olavide tratará los servicios, la información y los datos de carácter personal de los que sea responsable conforme a los siguientes principios de seguridad de la información y de privacidad:

a) Seguridad integral: la seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema. Quedan excluidas cualquier actuación puntual o tratamiento coyuntural. Se prestará la máxima atención a la concienciación de las personas que intervienen en el proceso y a sus responsables jerárquicos.

b) Gestión de riesgos: el análisis y gestión de riesgos será parte esencial del proceso de seguridad y deberá mantenerse permanentemente actualizado. La gestión del riesgo permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. Al evaluar el riesgo, la Universidad tendrá en cuenta los riesgos que se derivan para los derechos de las personas con respecto al tratamiento de sus datos personales.

c) Prevención, reacción y recuperación: la seguridad del sistema debe contemplar los aspectos de prevención, detección y corrección, para conseguir que la amenazas sobre el mismo no se materialicen, no afecten gravemente a la información que maneja ni a los servicios que se prestan.

d) Líneas de defensa: el sistema ha de disponer de una estrategia de protección constituida por múltiples capas de seguridad, que permita minimizar un posible impacto.

e) Mejora Continua: los procesos integrales de seguridad y de protección de datos, y en particular, las medidas de seguridad implementadas, se reevaluarán y actualizarán de forma continua, para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección, llegando incluso a un replanteamiento de dicho proceso, si fuese necesario.

f) Función diferenciada: en los sistemas de información de la Universidad se observará el principio de responsabilidad diferenciada de forma que se delimiten las diferentes responsabilidades y los roles.
g) Licitud, lealtad y transparencia: los datos de carácter personal serán tratados de manera lícita, leal y transparente en relación con el interesado.
h) Legitimación en el tratamiento de datos personales: solo se tratarán los datos de carácter personal cuando dicho tratamiento se encuentre amparado en alguna de las causas de legitimación establecidas en los artículos 6 y 9 del RGPD.
i) Limitación de la finalidad: los datos de carácter personal serán tratados para el cumplimiento de fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines.
j) Minimización de datos: los datos de carácter personal serán adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados.
k) Exactitud: los datos de carácter personal serán exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan.
l) Limitación del plazo de conservación: los datos de carácter personal serán mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines que justificaron su tratamiento.
m) Integridad y confidencialidad: los datos de carácter personal serán tratados de tal manera que se garantice su seguridad, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas. Quienes intervengan en el tratamiento de los datos estarán sujetos al deber de secreto incluso después de haber concluido aquel.
n) Atención de los derechos de los afectados: se adoptarán medidas en la organización que garanticen el adecuado ejercicio por los afectados, cuando proceda, de los derechos de acceso, rectificación, supresión, oposición, limitación del tratamiento y portabilidad respecto de sus datos de carácter personal.
o) Alcance estratégico: la seguridad de la información y la protección de datos deben contar con el compromiso y apoyo de todos los niveles directivos de forma que pueda estar coordinada e integrada con el resto de iniciativas estratégicas de la Universidad para conformar un todo coherente y eficaz.
p) Seguridad y privacidad desde el diseño: la Universidad promoverá que la seguridad de la información se aplique desde el diseño inicial de los sistemas de información. Asimismo, la Universidad promoverá la implantación del principio de protección de datos desde el diseño con el objetivo de cumplir los requisitos definidos en el RGPD y, por tanto, los derechos de los interesados de forma que la protección de datos se encuentre presente en las primeras fases de concepción de un proyecto.
q) Seguridad y privacidad por defecto: la Universidad promoverá que se contemplen los aspectos de seguridad de la información y privacidad en todas las fases del ciclo de vida de sus sistemas de información de forma que garanticen la seguridad de la información y la protección de datos por defecto. El sistema proporcionará la mínima funcionalidad requerida para que la organización alcance sus objetivos.
r) Responsabilidad proactiva: la Universidad será responsable del cumplimiento de los principios anteriormente señalados y del cumplimiento de la normativa legal vigente en materia de seguridad de la información y protección de datos, y adoptará las medidas técnicas, organizativas y procedimentales que le permitan estar en condiciones de demostrar dicho cumplimiento.

Las directrices fundamentales de seguridad de la información y protección de datos se concretan en un conjunto de requisitos mínimos y responsabilidades específicas que se configuran como objetivos instrumentales que garantizan el cumplimiento de los principios básicos de la Política de Seguridad de la Información y Protección de Datos y que inspiran las actuaciones de la Universidad en dichos ámbitos. Se establecen, como mínimos, los siguientes:

a) Registro de actividades de tratamiento y gestión de activos de información: se mantendrá un registro de actividades de tratamiento, en los términos previstos en el apartado "Registro de Actividades de Tratamiento" de esta Política, que se hará público en el portal de transparencia de la Universidad. Asimismo, los activos de información se encontrarán inventariados y categorizados y estarán asociados a un responsable.

b) Seguridad ligada a las personas: se implantarán los mecanismos necesarios para que cualquier persona que acceda, o pueda acceder a los activos de información y a los datos de carácter personal, conozca sus responsabilidades y de este modo se reduzca el riesgo derivado de un uso indebido de dichos activos.

c) La seguridad de los sistemas estará atendida, revisada y auditada por personal cualificado, dedicado e instruido en todas las fases de su ciclo de vida: instalación, mantenimiento, gestión de incidencias y desmantelamiento.

d) El personal recibirá la formación específica necesaria para garantizar la seguridad de las tecnologías de la información aplicables a los sistemas y servicios de la Administración.

e) Protección de las instalaciones: los activos de información serán emplazados en áreas seguras, protegidas por controles de acceso físicos adecuados a su nivel de criticidad. Los sistemas y los activos de información que contienen dichas áreas estarán suficientemente protegidos frente a amenazas físicas o ambientales.

f) Integridad y actualización del sistema: todo elemento físico o lógico requerirá autorización formal previa a su instalación en el sistema. Se deberá conocer en todo momento el estado de seguridad de los sistemas, en relación a las especificaciones de los fabricantes, a las vulnerabilidades y a las actualizaciones que les afecten, reaccionando con diligencia para gestionar el riesgo a la vista del estado de seguridad de los mismos.

g) Protección de información almacenada y en tránsito: la información que se transmita a través de redes de comunicaciones deberá ser adecuadamente protegida, teniendo en cuenta su nivel de sensibilidad y de criticidad, mediante mecanismos que garanticen su seguridad.
En la estructura y organización de la seguridad del sistema, se prestará especial atención a la información almacenada o en tránsito a través de entornos inseguros. Tendrán la consideración de entornos inseguros los equipos portátiles, móviles, tabletas, dispositivos periféricos, soportes de información y comunicaciones sobre redes abiertas o con cifrado débil.
El sistema ha de proteger el perímetro, en particular, si se conecta a redes públicas. En todo caso se analizarán los riesgos derivados de la interconexión del sistema, a través de redes, con otros sistemas, y se controlará su punto de unión;

h) Gestión de los incidentes de seguridad y privacidad: se implantarán los mecanismos apropiados para la correcta identificación, registro, resolución y notificación, en los términos previstos en las normativas de referencia en materia de seguridad y privacidad.

i) Se dispondrá de procedimientos de gestión de incidentes de seguridad, incidentes de privacidad y de debilidades detectadas en los elementos del sistema de información. Estos procedimientos cubrirán los mecanismos de detección, los criterios de clasificación, los procedimientos de análisis y resolución, así como los cauces de comunicación a las partes interesadas y el registro de las actuaciones. Este registro se empleará para la mejora continua de la seguridad del sistema.

j) Gestión de la continuidad: los sistemas dispondrán de copias de seguridad y se implantarán los mecanismos apropiados para asegurar la disponibilidad de los sistemas de información y mantener la continuidad de sus procesos de negocio, de acuerdo a las necesidades de nivel de servicio de sus usuarios.

BUPO N.º: 4/2019 Fecha de publicación: 04/10/2019

Control de Acceso y Registro de Actividad

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.

Se limitará el acceso a los activos de información por parte de usuarios, procesos y otros sistemas de información mediante la implantación de los mecanismos de identificación, autenticación y autorización acordes a la criticidad de cada activo. Además, quedará registrada la utilización del sistema con objeto de asegurar la trazabilidad del acceso y auditar su uso adecuado, conforme a la actividad de la organización.

Con la finalidad exclusiva de lograr el cumplimiento normativo, con plenas garantías del derecho al honor, a la intimidad personal y familiar y a la propia imagen de los afectados, y de acuerdo con la normativa sobre protección de datos personales, de función pública o laboral, y demás disposiciones que resulten de aplicación, se registrarán las actividades de los usuarios, reteniendo la información necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa.

Registro de Actividades de Tratamiento

La Universidad Pablo de Olavide mantendrá actualizado el registro de las actividades de tratamiento con datos de carácter personal de las que sea responsable, que incluirá toda la información a la que se refiere el artículo 30 del RGPD.

Conforme a lo establecido en el art. 31 de la LOPDGDD, la Universidad hará público en el portal de transparencia de la Universidad un inventario de sus actividades de tratamiento accesible por medios electrónicos en el que constará la información establecida en el artículo 30 del Reglamento (UE) 2016/679 y su base legal.

Todos los sistemas de información de la Universidad se ajustarán a los niveles de seguridad requeridos por la normativa para la naturaleza y finalidad de los datos de carácter personal recogidos en el mencionado listado de actividades de tratamiento. Dichas medidas de seguridad dependerán del análisis de riesgos realizado y tienen como objetivo mitigar el nivel de riesgo, basándose en medidas técnicas de seguridad, relacionadas con las medidas del ENS, y medidas jurídicas, relacionadas con los artículos del RGPD, de la LOPDGDD, o normas que los desarrollen.

BUPO N.º: 4/2019 Fecha de publicación: 04/10/2019

Análisis y Gestión de Riesgos y Evaluación de Impacto

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 servicios, de la información, 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.

Todos los sistemas afectados por esta Política están sujetos a un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá al menos una vez al año o cuando cambien la información manejada, los servicios prestados, suceda un incidente grave de seguridad o se detecten vulnerabilidades graves.

Para la armonización de los análisis de riesgos, la Comisión de Seguridad de la Información y Protección de Datos establecerá una valoración de referencia para los diferentes tipos de información manejada y los diferentes servicios prestados. La citada Comisión dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

La reducción de estos los niveles de riesgo se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los servicios, información o los tratamientos, de su valor, del impacto y de la probabilidad de los riesgos a los que estén expuestos y la eficacia y el coste de las medidas de seguridad.

Cuando la información contenga datos de carácter personal, se llevará a cabo, de forma periódica y al menos cada 2 años, un análisis de riesgos que permita identificar y gestionar los riesgos minimizándolos hasta los niveles que puedan considerarse aceptables. Esta evaluación incluirá un análisis de los riesgos para los derechos y libertades de las personas físicas respecto de las actividades de tratamiento con datos personales que lleve a cabo la Universidad, así como los sistemas de información que sirven de soporte para dichas actividades de tratamiento.

Asimismo, la Universidad llevará a cabo una evaluación de impacto de las actividades de tratamiento en la protección de datos personales cuando del análisis realizado resulte probable que el tratamiento suponga un riesgo significativo para los derechos y libertades de las personas, conforme a lo previsto en el artículo 35 del RGPD.

Notificación de Incidentes se Seguridad y Violaciones de Seguridad de los Datos de Carácter Personal

La Universidad Pablo de Olavide notificará los incidentes de seguridad a las autoridades públicas y equipos de respuesta competentes, de conformidad con lo dispuesto en la normativa que resulte de aplicación, adoptando las medidas de seguridad adecuadas y proporcionadas al nivel de riesgo determinado.

La Universidad, asimismo, adoptará las medidas necesarias para garantizar la notificación de las violaciones de seguridad de los datos de carácter personal que pudieran producirse a la autoridad de control competente, a través del procedimiento establecido al efecto, de conformidad con lo dispuesto en el artículo 33 del RGPD.

Igualmente adoptará las medidas procedentes para la comunicación a los interesados que pudieran haberse visto afectados por la violación de seguridad de los datos de carácter personal, conforme a lo dispuesto en el artículo 34 del RGPD.

Revisión y Auditoría

La Universidad llevará a cabo de forma periódica, y al menos cada dos años, una auditoría encaminada a la verificación, evaluación y valoración de la eficacia y el cumplimiento normativo de las medidas técnicas y organizativas para garantizar la seguridad de los tratamientos y sistemas de información.

En todo caso realizará una auditoría específica y extraordinaria cuando se lleven a cabo modificaciones sustanciales en el sistema de información que puedan repercutir en el cumplimiento de las medidas de seguridad implantadas.

Las auditorías serán supervisadas por el Responsable de Seguridad de la información y por el Delegado o Delegada de protección de datos.

Organización de la Seguridad de la Información y Protección de Datos

La estructura para la gestión de la seguridad de la información y la privacidad en el ámbito de la Política de la Seguridad de la Información y Protección de Datos de la Universidad Pablo de Olavide está compuesta por las siguientes figuras:

a) Comisión de Seguridad de la Información y Protección de Datos.
b) Responsable del Tratamiento.
c) Responsable de la Información.
d) Responsable del Servicio.
e) Responsable de la Seguridad de la Información.
f) Responsable del Sistema.
g) Administrador o Administradora de Seguridad del Sistema.
h) Delegado o Delegada de Protección de Datos.

Esta estructura será competente para mantener, actualizar y hacer cumplir la citada Política, dentro del alcance establecido por la misma.

Las distintas figuras individuales que integran esta estructura de seguridad y protección de datos, son designadas y nombradas formalmente mediante resolución del Rector o Rectora.

Comisión de Seguridad de la Información y Protección de Datos

Esta Comisión es un órgano colegiado de propuesta y seguimiento en materia de seguridad de los sistemas de información y protección de datos de carácter personal.

Está compuesta por los siguientes miembros:

- El vicerrector o vicerrectora competente en materia de Tecnologías de la Información y la Comunicación, en calidad de Responsable de Seguridad de la Información, que ejercerá la presidencia.
- El Secretario o Secretaria General, en calidad de Responsable de la Información y de Responsable del Tratamiento.
- El Gerente o la Gerente, en calidad de Responsable del Servicio.

- El Director o Directora del Servicio Administrativo con competencias en Administración Electrónica.
- El Director o Directora del Centro de Informática y Comunicaciones, en calidad de Responsable del Sistema.
- Los Jefes de Servicio del Centro de Informática y Comunicaciones.
- El Jefe o Jefa de Gestión de la Seguridad de la Información, en calidad de Administrador o Administradora de Seguridad del Sistema, que ejercerá las funciones de Secretario o Secretaria de la Comisión.
- El Delegado o Delegada de Protección de Datos de la Universidad participará, con voz, pero sin voto, en las reuniones cuando vayan a abordarse cuestiones relacionadas con el tratamiento de datos de carácter personal, así como siempre que se requiera su participación. En todo caso, si un asunto se sometiese a votación se hará constar siempre en acta su parecer.

Serán funciones de la Comisión de Seguridad de la Información y Protección de Datos:

a) Identificar, revisar y proponer objetivos estratégicos en materia de seguridad de la información y protección de datos.
b) Proponer y revisar la Política de Seguridad de la Información y Protección de Datos, así como las normas de seguridad y privacidad de ámbito global.
c) Asegurar la disponibilidad de los recursos necesarios para llevar a cabo los planes de acción relacionados con la seguridad de la información y la privacidad.
d) Proponer las iniciativas principales para mejorar la gestión de la seguridad de la información y la privacidad.
e) Realizar el seguimiento del nivel de seguridad de la información y la privacidad en base a unos indicadores definidos.
f) Conocer el resultado del análisis de riesgos y aprobar los umbrales de riesgo residual.

Además, desempeñará las siguientes funciones:

a) Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información, para asegurar que los esfuerzos son consistentes, que están alineados con la estrategia decidida en la materia, evitando duplicidades.
b) Velar porque la seguridad de la información y la privacidad se tenga en cuenta en todos los proyectos TIC desde su especificación inicial hasta su puesta en operación. En particular, deberá velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas TIC.
c) Promover recursos y medios para la concienciación y formación en materia de seguridad de la información y privacidad a todo el personal.

Responsable del Tratamiento y Responsable de la Información

La Universidad Pablo de Olavide será identificada como responsable respecto de aquellos tratamientos cuyos fines y medios sean determinados por esta Universidad. Esta condición le es atribuida como entidad con personalidad jurídica propia.

La Universidad Pablo de Olavide podrá ser identificada como corresponsable respecto de aquellos tratamientos cuyos fines y medios sean determinados por esta Universidad en concurso con otra persona o entidad, ya sea en virtud de convenio u otra fórmula procedente.

Fecha de publicación: 04/10/2019
BUPO N.º: 4/2019

Las competencias derivadas de la condición de Responsable del Tratamiento las asumirá el Secretario o Secretaria General de la Universidad y, en condición de tal, determinará los fines y medios del tratamiento de conformidad con lo dispuesto en el RGPD y en la LOPDGDD.

De igual manera, recae en el titular de dicho órgano la condición de Responsable de la Información en el ámbito del ENS y, en tal condición, tiene la responsabilidad de establecer los requisitos de la información en materia de seguridad de la información.

Son funciones del Responsable de la Información:

a) La determinación y aprobación formal de los niveles y medidas de seguridad de la información, a propuesta de la Comisión de Seguridad de la Información y Protección de Datos, dentro del marco de lo previsto en los Anexos I y II del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
b) En tanto que es el propietario de los riesgos sobre la información que le compete, aprobará formalmente el riesgo residual sobre la misma y será responsable de la monitorización del riesgo.
c) La aprobación, a propuesta de la Comisión de Seguridad de la Información y Protección de Datos, de las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo para los derechos y libertades de las personas, teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, conforme a lo exigido en el RGPD.

Son funciones del Responsable del Tratamiento:

a) Velar por el efectivo cumplimiento del RGPD, la LOPDGDD y la demás normativa vigente en el tratamiento de datos personales que se gestionan en la Universidad.
b) Organizar, mantener y dar publicidad a las actividades de tratamiento de datos de carácter personal.
c) Comunicar a la Delegada o al Delegado de Protección de Datos cualquier adición, modificación o exclusión en el contenido del registro.
d) Establecer y aplicar las medidas técnicas y organizativas de privacidad y seguridad necesarias para la protección de los datos personales en los tratamientos que gestiona la Universidad, que resulten apropiadas para garantizar un nivel de seguridad adecuado al riesgo, y para la aplicación efectiva de los principios de seguridad por defecto y desde el diseño.
e) Garantizar el cumplimiento de las obligaciones de secreto y confidencialidad derivadas de la normativa en materia de protección de datos personales en relación con los tratamientos que gestiona la Universidad.
f) Garantizar el cumplimiento de la obligación de informar adecuadamente y aplicando el principio de transparencia en la recogida de los datos personales.
g) Cumplir todas aquellas obligaciones y respetar los derechos de las personas interesadas, de acuerdo con lo previsto en el RGPD, la LOPDGDD y demás normativa vigente.
h) Realizar las pertinentes evaluaciones de impacto en la protección de datos, asesorado por la Delegada o el Delegado de Protección de Datos, cuando el tratamiento de datos a llevar a cabo entrañe alto riesgo para los derechos y libertades de las personas físicas. Si la evaluación de impacto mostrara que el tratamiento entraña alto riesgo, le corresponde realizar la consulta previa a la autoridad de control.
i) Definir las medidas necesarias para facilitar la detección de las incidencias de seguridad que afecten a los datos personales que se puedan producir y realizar, en su caso, las preceptivas notificaciones de violaciones de seguridad a la autoridad de control, a las personas interesadas y a la Delegada o el Delegado de Protección de Datos.

Fecha de publicación: 04/10/2019
BUPO N.º: 4/2019

j) Si el tratamiento, o parte de él, fuera realizado por un Encargado del tratamiento, el Responsable del Tratamiento elegirá únicamente un Encargado que ofrezca garantías suficientes para aplicar las medidas técnicas y organizativas apropiadas que le traslade de manera documentada. Así mismo, realizará seguimiento de la correcta aplicación de estas medidas.
k) La trasmisión de las obligaciones al Encargado del tratamiento y la verificación del cumplimiento de las mismas.
l) Autorizar las comunicaciones de datos a terceros que no estén amparadas por un requerimiento legal o que no resulten de la ejecución de un encargo de tratamiento.
m) Todas aquellas responsabilidades que exija la legislación vigente en materia de protección de datos de carácter personal y no estén atribuidas a ningún órgano.

Responsable del Servicio

Recae en el Gerente o la Gerente de la Universidad Pablo de Olavide la condición de Responsable del Servicio en el ámbito del ENS y, como tal, tiene como responsabilidad establecer los requisitos del servicio en materia de seguridad de la información.

Son funciones del Responsable del Servicio:

a) La determinación y aprobación formal de los niveles y medidas de seguridad de la información, a propuesta de la Comisión de Seguridad de la Información y Protección de Datos, dentro del marco de lo previsto en los Anexos I y II del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
b) En tanto que es el propietario de los riesgos sobre la información que le compete, aprobará formalmente el riesgo residual sobre la misma y será responsable de la monitorización del riesgo.
c) La aprobación, a propuesta de la Comisión de Seguridad de la Información y Protección de Datos, de las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo para los derechos y libertades de las personas, teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, conforme a lo exigido en el RGPD.

Específicamente en relación con los datos personales, son también funciones del Responsable del Servicio:

a) Prestar asistencia al Responsable del Tratamiento en el ejercicio de sus funciones.
b) Un tratamiento de información puede abarcar diferentes servicios y, por tanto, intervendrían en el tratamiento diferentes unidades administrativas y colectivos de personal y colaboradores. Deberá coordinarlos y asignar las responsabilidades y recursos que correspondan para el correcto ejercicio de sus funciones por parte del Responsable de la Información y Responsable del Tratamiento.

Responsable de Seguridad de la Información

Recae en el Vicerrector o Vicerrectora competente en materia de Tecnologías de la Información y la Comunicación de la Universidad Pablo de Olavide la condición de Responsable de Seguridad de la Información en el ámbito del ENS y, como tal, determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.

Fecha de publicación: 04/10/2019
BUPO N.º: 4/2019

Las responsabilidades del Responsable de Seguridad de la Información son:

a) Mantener el nivel adecuado de seguridad de la información manejada y de los servicios prestados por los sistemas.
b) Realizar o promover las auditorías periódicas a las que obliga el ENS para verificar el cumplimiento de los requisitos del mismo o cualquier otra auditoría de seguridad que sea necesaria.
c) Promover la formación y concienciación en materia de seguridad TI.
d) Realizar el análisis de riesgo de los sistemas y monitorizar que los sistemas de información se comportan dentro de los márgenes aceptados de riesgo.
e) Comprobar que las medidas de seguridad existentes son las adecuadas para las necesidades de la Universidad. Analizar y promover salvaguardas de seguridad.
f) Elaborar y firmar el documento de Declaración de Aplicabilidad.
g) Constituirse como punto de contacto con las autoridades competentes en materia de seguridad de la información. En particular, para coordinarse con el CESIRT de referencia, recopilando, preparando y suministrando la información solicitada o enviada a iniciativa propia y notificando, en los casos y términos que la legislación establezca, sin dilación indebida, aquellos incidentes de seguridad que deban ser reportados.
h) Revisar y aprobar toda la documentación relacionada con la seguridad del sistema.
i) Proponer los riesgos, a los propietarios de los riesgos, para su aprobación formal.
j) Apoyar y supervisar la investigación de los incidentes de seguridad desde su notificación hasta su resolución, emitiendo informes periódicos sobre los más relevantes al Consejo de Dirección de la Universidad.
k) Reportar al Consejo de Dirección de la Universidad sobre el estado general de la Seguridad de la Información.

El Responsable de la Seguridad de la Información determinará qué medidas de seguridad física deberán ser adoptadas por el responsable de la Universidad competente en la materia de Seguridad Física, quien además deberá informar al Responsable de Seguridad de la Información de su grado de implantación, eficiencia y de los incidentes relacionados con dichas medidas.

El Responsable de la Seguridad de la Información determinará qué medidas deberán ser adoptadas por el órgano responsable de la gestión del personal en el ámbito de sus competencias, quien además deberá informar al Responsable de Seguridad de la Información de su grado de implantación, eficiencia y de los incidentes relacionados con dichas medidas.

Responsable del Sistema

Recae en el máximo responsable del Servicio competente en Tecnologías de la Información la condición de Responsable del Sistema y, como tal, tiene como responsabilidad las siguientes tareas propias de la operación de los sistemas de información:

a) Desarrollar y gestionar el Sistema durante todo su ciclo de vida, desde la especificación, instalación hasta el seguimiento de su funcionamiento.
b) Definir la topología y sistema de gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo.
c) Aprobar los cambios que afecten a la seguridad del modo de operación del Sistema.
d) Determinar la configuración autorizada de hardware y software a utilizar en el Sistema y aprobar las modificaciones importantes de dicha configuración.
e) Elaborar la documentación de seguridad del Sistema.
f) Elaborar procedimientos operativos de seguridad.
g) Implantar y controlar las medidas específicas de seguridad del Sistema y cerciorarse de que las medidas de seguridad se integren adecuadamente en el marco general de seguridad
h) Establecer planes de contingencia y emergencia, llevando a cabo frecuentes ejercicios para que el personal se familiarice con ellos.

Fecha de publicación: 04/10/2019
BUPO N.º: 4/2019

i) Elaborar planes de mejora de la seguridad y ejecutar el plan de mejora de la seguridad aprobado. Planificar la implementación de salvaguardas.
j) Acordar la suspensión del manejo de cierta información o la prestación de un cierto servicio si detecta deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. La decisión final, que será tomada por la dirección de la entidad, debe ser acordada con los responsables de la información y los servicios afectados y el Responsable de la Seguridad.

Administrador de la Seguridad del Sistema

Recae en el Jefe o Jefa de Gestión de Seguridad la condición de Administrador de Seguridad del Sistema y, como tal, tiene como responsabilidad la implantación, gestión y mantenimiento de las medidas de seguridad aplicables al sistema de información.

Las responsabilidades del Administrador de la Seguridad del Sistema son:

a) La implementación, gestión y mantenimiento de las medidas de seguridad aplicables al Sistema de Información.
b) La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad del Sistema de Información.
c) La gestión de las autorizaciones y privilegios concedidas a los usuarios del sistema, en particular los privilegios concedidos, incluyendo la monitorización de que la actividad desarrollada en el sistema se ajusta a lo autorizado.
d) La aplicación de los Procedimientos Operativos de Seguridad.
e) Asegurar que los controles de seguridad establecidos son adecuadamente observados.
f) Asegurar que son aplicados los procedimientos aprobados para manejar el sistema de información.
g) Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida y que en todo momento se ajustan a las autorizaciones pertinentes.
h) Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica implementados en el sistema.
i) Informar al Responsable de la Seguridad y del Sistema de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.
j) Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución. Llevar a cabo el registro, contabilidad y gestión de los incidentes de seguridad en los sistemas de información bajo su responsabilidad.

Encargado de Tratamiento

Cuando la Universidad Pablo de Olavide sea Responsable de Tratamiento, la condición de Encargado de Tratamiento será atribuible a la persona o entidad que, en su caso, trate los datos personales por cuenta de la Universidad Pablo de Olavide.

El tratamiento por el Encargado se regirá por un contrato u otro acto jurídico con arreglo al Derecho de la Unión o de los Estados miembros, que vincule al Encargado respecto del responsable y establezca el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable. Dicho contrato o acto jurídico estipulará, en particular, que el Encargado adquiera las responsabilidades establecidas en el artículo 28 del RGPD.

Fecha de publicación: 04/10/2019
BUPO N.º: 4/2019

Cuando se contraten con terceros determinadas actividades que comporten el tratamiento de datos personales, el Encargado del Tratamiento, en la parte que le corresponda, podrá asumir eventualmente la figura de Responsable del Sistema (con una responsabilidad inmediata sobre el mismo, dado que la responsabilidad mediata corresponde a la Universidad). Como tal, eventualmente podrá ser invitado a participar en la Comisión de Seguridad y Protección de Datos, si el Responsable de Seguridad lo estima conveniente, en función de la entidad del sistema de información y de los datos tratados.

La Universidad Pablo de Olavide también podrá ostentar la condición de Encargado de Tratamiento cuanto trate datos por cuenta de un Responsable. Esta condición le es atribuida como entidad con personalidad jurídica propia.

La condición de Encargado debe constar en los actos que formalicen o resulten del tratamiento, atribuyéndose tal condición a la Universidad o entidad correspondiente.

Delegado o Delegada de Protección de Datos

El Delegado o Delegada de Protección de Datos tiene como responsabilidad coordinar e implantar las medidas de seguridad técnicas, organizativas y jurídicas en materia de protección de datos personales.

La Universidad Pablo de Olavide cuenta con una persona que ocupa el puesto de Delegado de Protección de Datos, a fin de dar cumplimiento a lo requerido en el artículo 37 del RGPD, que llevará a cabo las tareas establecidas en el artículo 39 del citado RGPD, así como las que se deriven de la normativa española de protección de datos de carácter personal y normativa de desarrollo.

Resolución de Conflictos

En caso de conflicto entre los diferentes responsables que componen la estructura organizativa de la Política de Seguridad de la Información y Protección de Datos corresponderá, en última instancia, al Rector o Rectora la resolución de los mismos, en calidad de máximo responsable de la institución. A estos efectos, será asistido por cualquiera de las figuras que participan en la estructura de seguridad de la información y protección de datos.

Obligaciones del Personal

Todos los miembros de la Universidad tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y Protección de Datos, así como las normativas y procedimientos que las desarrollen.

Todo el personal que presta servicio en la Universidad tiene asimismo el deber de colaborar en la mejora de los principios y requisitos en materia de seguridad de la información y protección de datos evitando y aminorando los riesgos a los que se encuentra expuestos los servicios, la información y los datos personales de los que es titular la Universidad. A tal efecto, comunicarán a los integrantes de la estructura organizativa de la Política de Seguridad de la Información y Protección de Datos cualquier propuesta o sugerencia que ayude a preservar la confidencialidad, la integridad y la disponibilidad de los servicios y la información.

Todos los órganos y unidades de la Universidad prestarán su colaboración en las actuaciones de implementación de la Política de Seguridad de la Información y Protección de Datos.

Las personas con responsabilidad en el uso, operación o administración de sistemas TIC recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo. La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

Formación y Concienciación

El objetivo es lograr la plena conciencia respecto a que la seguridad de la información y la protección de los datos de carácter personal afecta a todo el personal de la Universidad y a todas las actividades, de acuerdo al principio de seguridad integral recogido en el art. 5 del ENS y a la responsabilidad de la Universidad en la aplicación de medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, de conformidad con el art. 32 del RGPD y la Disposición Adicional Primera de la LOPDGDD, entre otros preceptos.

A estos efectos, la Universidad, propondrá y organizará sesiones formativas y de concienciación para que todas las personas que intervienen en el proceso y sus responsables jerárquicos sean conscientes de la relevancia de la seguridad de la información y, en particular, de la protección de los datos personales, y de la importancia de asegurar el cumplimiento de la Política de Seguridad de la Información y Protección de Datos, así como las normativas y procedimientos que la desarrollen, al objeto de proteger los servicios, la información y los datos personales que trata y gestiona la Universidad de los diferentes riesgos y amenazas a la que está expuesta.

Responsabilidades en Caso de Incumplimiento

La Comisión de Seguridad de la Información y Protección de Datos, en casos de incumplimiento de las obligaciones previstas en la Política de Seguridad de la Información y de Protección de Datos, o en las normativas y procedimientos que la desarrollen, propondrá al órgano competente la adopción de medidas preventivas y correctoras encaminadas a salvaguardar y proteger las redes y sistemas de información.

Si la Comisión entendiera que el personal, en el acceso o tratamiento de datos en el ejercicio de sus actividades profesionales, pudiera haber incurrido en un incumplimiento de la Política de Seguridad de la Información y Protección de Datos, instará por los cauces establecidos, la depuración de las responsabilidades disciplinarias a las que hubiera lugar. El procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario del personal al servicio de las Administraciones Publicas o de la propia Universidad Pablo de Olavide.

Terceras Partes

Cuando la Universidad preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipes de esta Política de Seguridad de la Información y Protección de Datos, se establecerán canales para reporte y coordinación de los respectivos Comités o Comisiones, o responsables con competencias en Seguridad de la Información y de Protección de Datos y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad y violaciones de seguridad que afecten a datos de carácter personal.

Cuando la Universidad utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad de la Información y Protección de Datos y de la Normativa de Seguridad que ataña a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias. Se garantizará que el personal de terceros esté adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política.

Fecha de publicación: 04/10/2019
BUPO N.º: 4/2019

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

Las aplicaciones que se desarrollen para la Universidad Pablo de Olavide deberán contemplar aspectos de seguridad de la información y la privacidad 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.

Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por el Responsable de la Información y el Responsable del Servicio antes de seguir adelante.

Para la contratación de servicios de seguridad se estará a lo dispuesto en el artículo 15 y en el artículo 18 del ENS.

La Universidad exigirá, de manera objetiva y no discriminatoria, que las organizaciones que les presten servicios de seguridad cuenten con profesionales cualificados y con unos niveles idóneos de gestión y madurez en los servicios prestados.

Aprobación y Desarrollo de la Política de Seguridad de la Información y Protección de Datos

Corresponde al Rector o Rectora de la Universidad Pablo de Olavide la aprobación y difusión de la Política de Seguridad de la Información y Protección de Datos, a propuesta por la Comisión de Seguridad y Protección de Datos.

La citada Comisión revisará la Política como mínimo una vez al año.

Esta Política se desarrollará por medio de documentos más precisos que ayuden a materializar sus contenidos, mediante los que se adopten 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. Estas medidas técnicas y organizativas podrán plasmarse en:

- Normas de seguridad: estas normas uniformizan el uso de aspectos concretos del sistema, indican los usos correctos y las responsabilidades de los usuarios.
- Procedimientos de seguridad y/o de protección de datos: conjunto de documentos que describen explícitamente y paso a paso cómo realizar una cierta actividad.
- Documentos formativos u orientativos: documentación de buenas prácticas, recomendaciones, guías, material de formación, presentaciones, entre otros.

Las normas serán de carácter obligatorio y serán propuestas y revisadas por la Comisión de Seguridad de la Información y Protección de Datos, y aprobadas por el Consejo de Gobierno, o por el Rector o Rectora (u órgano en quien delegue), en función de su alcance y de la forma que revistan las decisiones mediante las que se adoptan (reglamentos, instrucciones, circulares, u otros).

Los procedimientos y otros documentos serán aprobados por los responsables que corresponda de la organización de seguridad de la información y protección de datos establecido en la presente Política, en función de su ámbito de aplicación. Si dicho ámbito afecta a varios responsables, deberán ser aprobados por todos ellos.

Estos documentos estarán a disposición de todos los miembros de la organización que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

BUPO N.º: 4/2019 Fecha de publicación: 04/10/2019

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.

- Datos personales. Toda información sobre una persona física identificada o identificable ("el interesado"); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.

- 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.

- 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.

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

- 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 y, en particular, sobre los tratamientos de datos de carácter personal, 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 de la información y Protección de Datos. Documento escrito que contiene de forma conjunta:

    - Conjunto de directrices que rigen la forma en que una organización gestiona y protege la información y los servicios que se consideran críticos, así como los datos de carácter personal que gestiona.

    - Identificación de las responsabilidades en el cumplimiento de la normativa vigente en materia de seguridad de la información y protección de datos de carácter personal.

- 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.

- Tratamiento. Cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción

Fecha de publicación: 04/10/2019

BUPO N.º: 4/2019