UNIVERSIDAD DE MÁLAGA

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE LA UNIVERSIDAD DE MÁLAGA

Preámbulo

La Universidad de Málaga dispone de sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar sus objetivos como organización. 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.

Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, uso previsto y valor de la información y los servicios. Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios. Es por ello por lo que el Esquema Nacional de Seguridad (Real Decreto 3/2010 de 8 de enero, ENS en adelante), en su artículo 11 establece que "Todos los órganos superiores de las Administraciones Públicas deberán disponer formalmente de su Política de Seguridad, que será aprobada por el titular del órgano superior correspondiente".

Esto implica que las diferentes áreas de la UMA deben aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad, así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

Todas las áreas deben actuar para que la seguridad TIC sea una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y las necesidades de financiación deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos de TIC. Las áreas deben estar preparadas para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo con el Artículo 7 del ENS.

Por todo ello, la UMA establece como objetivos de la seguridad de la información los siguientes:

- Cumplir la legislación de seguridad y privacidad.
- Garantizar la calidad y protección de la información.
- Garantizar la prestación continuada de los servicios.
- Lograr la plena concienciación de los usuarios respecto a la seguridad de la información.

TÍTULO I

Disposiciones generales

Artículo 1

Objeto y ámbito de aplicación

La presente Política de Seguridad afecta a las diferentes actividades en las que participa la UMA a través de medios electrónicos, en concreto:

a) Las relaciones entre los estudiantes, PAS, PDI y la propia UMA.

b) La consulta, por parte de sus colectivos, de la información pública administrativa y de los datos administrativos que estén en poder de la UMA.

c) La realización de los trámites y procedimientos administrativos incorporados para su tramitación en la Sede Electrónica.

d) El tratamiento de la información obtenida por la UMA en el ejercicio de sus potestades.

En consecuencia, esta política se aplica a todos los sistemas TIC a todos los miembros de la comunidad universitaria, sin excepciones.

Artículo 2

Marco normativo

El marco legal en materia de seguridad de la información viene establecido por la siguiente legislación:

- 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 (RGPD).
- Ley orgánica 3/2018 de 5 de diciembre, de protección de datos y garantía de derechos digitales.
- Ley 39/2015 de 1 de octubre, de Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 40/2015 de 1 de octubre, de Régimen Jurídico del Sector Público.
- El Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad.
- Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad.
- Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad.

Artículo 3

Principios básicos de protección

Los principios básicos son directrices fundamentales de seguridad que han de tenerse siempre presentes en cualquier actividad relacionada con el uso de los activos de información. Se establecen los siguientes:

a) **Alcance estratégico:** La seguridad de la información debe 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 para conformar un todo coherente y eficaz.

b) **Responsabilidad diferenciada:** En los sistemas de información se diferenciará el responsable de la información, que determina los requisitos de seguridad de la información tratada; el responsable del servicio, que determina los requisitos de seguridad de los servicios prestados; el responsable del sistema, que tiene la responsabilidad sobre la prestación de los servicios y el responsable de seguridad, que determina las decisiones para satisfacer los requisitos de seguridad.

c) **Seguridad integral:** La seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema, evitando, salvo casos de urgencia o necesidad, cualquier actuación puntual o tratamiento coyuntural. La seguridad de la información debe considerarse como parte de la operativa habitual, estando presente y aplicándose desde el diseño inicial de los sistemas de información.

d) **Gestión de Riesgos:** El análisis y gestión de riesgos será parte esencial del proceso de seguridad. La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, el impacto y la probabilidad de los riesgos a los que estén expuestos y la eficacia y el coste de las medidas de seguridad. Al evaluar el riesgo en relación con la seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales.

e) **Proporcionalidad:** El establecimiento de medidas de protección, detección y recuperación deberá ser proporcional a los potenciales riesgos y a la criticidad y valor de la información y de los servicios afectados.

f) **Mejora continua:** Las medidas de seguridad se reevaluarán y actualizarán periódicamente para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección. La seguridad de la información será atendida, revisada y auditada por personal cualificado, instruido y dedicado.

g) **Seguridad por defecto:** Los sistemas deben diseñarse y configurarse de forma que garanticen un grado suficiente de seguridad por defecto.

Artículo 4
Directrices fundamentales de protección

Las directrices fundamentales de seguridad se concretan en un conjunto de principios particulares y responsabilidades específicas, que se configuran como objetivos instrumentales que garantizan el cumplimiento de los principios básicos de la Política de Seguridad. Se establecen los siguientes:

a) Protección de datos de carácter personal: Se adoptarán las medidas técnicas y organizativas que corresponda implantar para atender los riesgos generados por el tratamiento de acuerdo a lo exigido por el citato Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.

b) Gestión de activos de información: Los activos de información se encontrarán inventariados y categorizados y estarán asociados a un responsable.

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

d) Seguridad física: 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.

e) Seguridad en la gestión de comunicaciones y operaciones: Se establecerán los procedimientos necesarios para lograr una adecuada gestión de la seguridad, operación y actualización de las Tecnologías de la Información y Comunicaciones. 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.

f) Control de acceso: 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 universitaria.

g) Adquisición, desarrollo y mantenimiento de los sistemas de información: Se contemplarán los aspectos de seguridad de la información en todas las fases del ciclo de vida de los sistemas de información, garantizando su seguridad por defecto.

h) Gestión de los incidentes de seguridad: Se implantarán los mecanismos apropiados para la correcta identificación, registro y resolución de los incidentes de seguridad.

i) Gestión de la continuidad: 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.

j) Cumplimiento: Se adoptarán las medidas técnicas, organizativas y procedimentales necesarias para el cumplimiento de la normativa legal vigente en materia de seguridad de la información.

TÍTULO II

Organización de la Seguridad

Capítulo I

Roles y funciones

Artículo 5

Definición de roles

La Política de Seguridad, según detalla el Anexo II del ENS, en su sección 3.1, debe identificar unos claros responsables para velar por su cumplimiento y ser conocida por todos los miembros de la organización. Los diferentes roles de seguridad de la información (autoridad principal y posibles delegadas) se limitan a una jerarquía simple: el Comité de Seguridad de la Información y la Privacidad da instrucciones al Responsable de la Seguridad de la Información que se encarga de cumplimentar, supervisando que administradores y operadores implementan las medidas de seguridad según lo establecido en la política de seguridad aprobada. Por su parte el Delegado de Protección de Datos debe ser oído en todos los aspectos relacionados con la seguridad de los datos personales y violaciones de seguridad de datos personales, entendiendo las mismas desde la perspectiva de la confidencialidad, integridad y disponibilidad.

Artículo 6

Composición del Comité de Seguridad de la Información y la Privacidad

El Comité de Seguridad de la Información y la Privacidad coordina la seguridad de la información a nivel de la universidad. Estará compuesto por los siguientes miembros:

Presidente	Rector	Delega en el VR con competencias en materia de Tecnologías de la Información y la Comunicación
Secretario	Vicesecretario General	Vicesecretario General
Vocales	Responsable de Información	Gerente

		Vicegerente Organización
	Responsable de Servicio	Vicerrector PDI
		Vicerrector Estudiantes
	Responsable de Seguridad	Director Técnico del SCI
	Responsable de Sistemas	Jefe de Servicio de Sistemas y Comunicaciones
		Jefe de Servicio de Desarrollo de Aplicaciones
	Responsable de Gestión de Personal	Vicegerente RRHH
	Administrador de Seguridad	Gestor de Seguridad del SCI
Asesor / Consejero	Delegado de Protección de Datos	Delegado de Protección de Datos
	Asesor jurídico	Asesor jurídico de la UMA

A requerimiento del Comité se convocará a cualquier miembro de la comunidad universitaria, cuya intervención sea precisa.

Artículo 7

Funciones del Comité

Corresponde al Comité de Seguridad de la Información y la Privacidad:

- Atender las inquietudes que le sean trasladadas, tanto por los órganos de dirección como por los diferentes centros, departamentos o servicios de la UMA.
- Informar regularmente del estado de la seguridad de la información al Consejo de Dirección.
- Promover la mejora continua del Sistema de Gestión de la Seguridad de la Información.
- Promover la realización de las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones de la universidad en materia de seguridad.
- Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información, para asegurar que los esfuerzos son consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades.
- Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables y/o entre diferentes áreas de la UMA, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.
- Revisar la Política de Seguridad de la información para que sea aprobada por el Consejo de Gobierno.
- Elaborar la estrategia de evolución de la UMA en lo que respecta a la seguridad de la información.
- Aprobar la normativa de seguridad de la información.
- Elaborar y aprobar los requisitos de formación y cualificación de administradores, operadores y usuarios desde el punto de vista de seguridad de la información
- Aprobar planes de mejora de la seguridad de la información de la UMA. En particular, velará por la coordinación de diferentes planes que puedan realizarse en diferentes áreas.
- Monitorizar los principales riesgos residuales asumidos por la UMA y recomendar posibles actuaciones respecto de ellos.
- Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones respecto de ellos. En particular, velar por la coordinación de las diferentes áreas de seguridad en la gestión de incidentes de seguridad de la información.

- Velar para que la seguridad de la información se tenga en cuenta en todos los proyectos TIC desde su especificación inicial hasta su puesta en operación.

Artículo 8

Funciones de la dirección política de la Universidad en materia de seguridad

La función de dirección política en materia de seguridad le corresponderá al rector, que podrá delegarla en el vicerrector con competencias en materia de tecnologías de la información y la comunicación, que estará a su vez apoyado por el Consejo de Dirección, que es el órgano que define la misión de la UMA, determina los objetivos que se propone alcanzar y se responsabiliza de su consecución. Son sus funciones:

- Aprobar el Plan de Adecuación al ENS.
- Aprobar la Política de Seguridad, así como las revisiones de la misma.
- Aprobar los planes de tratamiento del riesgo
- Proporcionar los recursos necesarios

Artículo 9

Funciones del Secretario/a

Corresponde al Secretario/a del Comité de Seguridad de la Información y la Privacidad:

- Convocar las reuniones del Comité.
- Preparar los temas a tratar en las reuniones del Comité, aportando información puntual para la toma de decisiones.
- Elaborar el acta de las reuniones.
- La responsabilidad de la ejecución directa o delegada de las decisiones del Comité.

Artículo 10

Funciones de los Vocales

Corresponde a los vocales del Comité de Seguridad de la Información y la Privacidad:

- Participar en las reuniones.
- Contribuir con ideas y sugerencias para el buen desarrollo de las reuniones.

Artículo 11

Funciones del Delegado de Protección de Datos

Corresponde al Delegado de Protección de Datos asesorar en aquellos aspectos que afecten a la seguridad de los datos personales y violaciones de seguridad de los datos personales:

- Participar en las reuniones.
- Emitir su parecer en aquellos aspectos relacionados con la seguridad de los datos personales, promover, en su caso, revisiones de análisis de riesgos, elaboración de evaluaciones de impacto en protección de datos, elaboración o modificación de procedimientos o políticas de seguridad de datos personales, entre otros.

Artículo 12

Funciones del Responsable de la Información

Las funciones del Responsable de la Información son las siguientes:

- Establecer los requisitos de la información en materia de seguridad. En el marco del ENS, equivale a la potestad de determinar los niveles de seguridad de la información.
- Determinar los niveles de seguridad en cada dimensión (confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad) dentro del marco establecido en el Anexo I del Esquema Nacional de Seguridad.
- Adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.
- Solicitar opinión al Delegado de Protección de Datos y a Responsable de Seguridad sobre las violaciones de seguridad de datos personales y en su caso, recomendar la notificación a la Agencia Española de Protección de Datos y /o a los propios interesados.

Tiene la responsabilidad última del uso que se haga de una cierta información y, por tanto, de su protección y de cualquier error o negligencia que lleve a un incidente de confidencialidad o de integridad.

Artículo 13

Funciones del Responsable del Servicio

Las funciones del Responsable del Servicio son las siguientes:

- Tiene la responsabilidad última del uso que se haga de determinados servicios y, por tanto, de su protección.
- Tiene la potestad de establecer los requisitos del servicio en materia de seguridad o, en terminología del ENS, la potestad de determinar los niveles de seguridad de los servicios.
- Aprobar el riesgo residual (el resultante una vez aplicados los controles de seguridad).
- En cuanto al Reglamento 2016/679 General de Protección de Datos, por delegación del Responsable del Tratamiento, se encomienda al Responsable del Servicio el desarrollo de las tareas relacionadas con la gestión de los tratamientos de datos personales que se realizan en su área en concreto.

Artículo 14

Funciones del Responsable de Seguridad

Las funciones del Responsable de Seguridad son las siguientes:

- Participar en la elaboración, en el marco del Comité de Seguridad de la Información y la Privacidad, de la Política y Normativa de Seguridad de la Información, para su aprobación por la Dirección.
- Elaborar y aprobar los Procedimientos Operativos de Seguridad de la Información.
- Coordinar la realización de un análisis de riesgos, así como la efectiva implementación de los controles previstos para eliminar o reducir el riesgo.
- Reportar al Delegado de Protección de Datos, al Responsable de Información y al Comité de Seguridad las violaciones de seguridad de los datos personales.
- Promover la formación y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad.
- Elaborar los Planes de Formación y Concienciación del personal en Seguridad de la Información, que deberán ser aprobados por el Comité de Seguridad de la Información y la Privacidad

- Mantener la seguridad de la información y de los servicios prestados por los sistemas de información en su ámbito de responsabilidad, de acuerdo a lo establecido en la Política de Seguridad de la UMA.
- Recopilar los requisitos de seguridad de los Responsables de Información y Servicio y determinar la categoría del Sistema.
- Facilitar a los Responsable de Información y a los Responsables de Servicio información sobre el nivel de riesgo residual esperado tras implementar las opciones de tratamiento seleccionadas en el análisis de riesgos y las medidas de seguridad requeridas por el ENS.
- Elaborar, junto a los Responsables de Sistemas, Planes de Mejora de la Seguridad, para su aprobación por el Comité de Seguridad de la Información y la Privacidad.
- Aprobar las directrices propuestas por los Responsables de Sistemas para considerar la Seguridad de la Información durante todo el ciclo de vida de los activos y procesos: especificación, arquitectura, desarrollo, operación y cambios.
- Facilitar periódicamente al Comité de Seguridad un resumen de actuaciones en materia de seguridad, de incidentes relativos a seguridad de la información y del estado de la seguridad de sistema (en particular del nivel de riesgo residual al que está expuesto el sistema).

Artículo 15

Funciones del Responsable del Sistema

Las funciones del Responsable del Sistema son las siguientes:

- Desarrollar, operar y mantener el Sistema de Información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.
- Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.
- Acordar la suspensión del manejo de una cierta información o la prestación de un cierto servicio si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos.
- Definir la topología y sistema de gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Definir la política de conexión o desconexión de equipos y usuarios nuevos en el Sistema.
- Decidir las medidas de seguridad que aplicarán los suministradores de componentes del Sistema durante las etapas de desarrollo, instalación y prueba del mismo.
- Determinar la configuración autorizada de hardware y software a utilizar en el Sistema.
- Elaborar procedimientos operativos de seguridad.
- Establecer planes de contingencia y emergencia, llevando a cabo frecuentes ejercicios para que el personal se familiarice con ellos.
- Aprobar los cambios que afecten a la seguridad del modo de operación del Sistema.
- Aprobar toda modificación sustancial de la configuración de cualquier elemento del Sistema.
- Monitorizar el estado de la seguridad del Sistema de Información y reportarlo periódicamente o ante incidentes de seguridad relevantes al Responsable de Seguridad de la Información.
- Comunicar tan pronto como se tenga constancia de la misma al Responsable de Seguridad las violaciones de seguridad que afecten a datos personales.

Artículo 16

Funciones del Responsable de Gestión del Personal

Le corresponde implantar las medidas de seguridad que le competan dentro de las determinadas por el Responsable de Seguridad de la Información, e informará a éste de su grado de implantación, eficacia e incidentes.

Artículo 17

Funciones del Administrador de Seguridad

Las funciones del Administrador de la Seguridad del Sistema son las siguientes:

- La implementación, gestión y mantenimiento de las medidas de seguridad aplicables al Sistema de Información.
- Asegurar que los controles de seguridad establecidos son cumplidos estrictamente.
- Informar a los Responsables de la Seguridad y del Sistema de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.
- Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución.
- 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.
- Aprobar los cambios en la configuración vigente del Sistema de Información.
- 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.
- La gestión de las autorizaciones 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.
- La aplicación de los Procedimientos Operativos de Seguridad.
- Asegurar que son aplicados los procedimientos aprobados para manejar el sistema de información.
- 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.
- Comunicar tan pronto como se tenga constancia de la misma al Responsable de Seguridad las violaciones de seguridad que afecten a datos personales.

Artículo 18

Resolución de conflictos

En caso de conflicto entre los diferentes responsables que componen la estructura organizativa de la Política de Seguridad prevalecerá la decisión del Comité de Seguridad de la Información y la Privacidad.

Capítulo II

Obligaciones y formación del personal

Artículo 19

Obligaciones del personal

Los miembros de la UMA tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad, siendo responsabilidad del Comité de Seguridad de la Información y la Privacidad disponer los medios necesarios para que la información llegue a los afectados.

Artículo 20

Formación y concienciación

Se desarrollarán actividades formativas específicas orientadas a la concienciación y formación de los empleados públicos de la UMA, así como a la difusión entre los mismos de la Política de seguridad y de su desarrollo normativo.

Artículo 21

Cumplimiento de la Política

El cumplimiento de la presente Política de Seguridad es obligatorio por parte de todo el personal interno o externo que intervenga en los procesos la UMA.

Artículo 22

Terceras partes

Cuando se utilicen servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad 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.

Capítulo III

Revisión y aprobación

Artículo 23

Revisión de la Política de Seguridad

La Política de Seguridad de la Información será revisada por el Comité de Seguridad de la Información y la Privacidad a intervalos planificados, o siempre que se produzcan cambios significativos, a fin de asegurar que se mantenga su idoneidad, adecuación y eficacia.