Proyecto de Reglamento X/2024, de XX de xxxxxx, por el que se regula la Política de Seguridad de la Información de la Universidad de Málaga

PREÁMBULO

La Ley Orgánica 2/2023, de 22 de marzo, del Sistema Universitario, en el artículo 33, apartado m), reconoce el derecho a la seguridad de los medios digitales y a la garantía de los derechos fundamentales en internet.

Los Estatutos de la Universidad de Málaga, aprobados mediante Decreto 464/2019, de 14 de mayo, en su disposición adicional quinta, dedicada a la transparencia y la protección de datos, atribuye a la Universidad de Málaga el compromiso de reforzar la protección de los datos personales, de conformidad con la legislación europea y estatal, así como el regular y garantizar el derecho de acceso a la información relativa a aquella actividad y establecer las obligaciones de buen gobierno que deberán cumplir las personas integrantes de sus órganos de gobierno. A su vez, en su disposición adicional séptima, regula el funcionamiento electrónico de la Universidad, fijando el compromiso de la Universidad de Málaga, como integrante del sector público institucional, de implantar y desarrollar la Administración electrónica, a través de su portal de internet, creando la sede electrónica, el registro electrónico y un archivo electrónico único, junto a la adopción de las medidas necesarias para garantizar la actuación administrativa automatizada, la firma electrónica del personal al servicio de la Universidad de Málaga y el intercambio electrónico de datos, fomentando la interoperabilidad con las Administraciones públicas.

Por su parte, la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, dedica su artículo 156 al Esquema Nacional de Seguridad, refiriéndose al mismo, en su apartado 2, como aquel que tiene por objeto establecer la política de seguridad en la utilización de medios electrónicos en el ámbito de la propia Ley, y que se encuentra constituido por los principios básicos y requisitos mínimos que garanticen adecuadamente la seguridad de la información tratada.

En desarrollo del marco legal citado, el Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos, en su anexo, ofrece un conjunto de definiciones que perfilan y clarifican, entre otros, qué ha de entenderse por Esquema Nacional de Seguridad, conceptuándolo como el "instrumento que tiene por objeto establecer la política de seguridad en la utilización de medios electrónicos en el ámbito de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público y está constituido por los principios básicos y requisitos mínimos que garanticen adecuadamente la seguridad de la información tratada".

Las Tecnologías de la Información y las Comunicaciones (TIC) juegan un papel fundamental hoy día en la prestación de servicios en la Administración Pública y en el ámbito universitario y cada vez se hace más necesaria su adecuada gestión y protección, ya que de ellas depende que la Universidad pueda desempeñar sus fines de forma efectiva. Además, con el inexorable contexto de transformación digital en el que nos encontramos, la información se convierte en uno de los activos más importantes de la Universidad de Málaga,

y como tal, debemos de protegerla con sistemas que garanticen la seguridad de la misma, así como la continuidad en la prestación de los servicios universitarios.

Consecuentemente, los sistemas TIC deben estar protegidos contra amenazas que están en rápida evolución. 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 (ENS), aprobado mediante el Real Decreto 311/2022, de 3 de mayo, en su artículo 12.2. establece que "Cada Administración pública contará con una política de seguridad formalmente aprobada por el órgano competente".

El Anexo II del ENS determina que esta política de seguridad se plasmará en un documento en el que, de forma clara, se precise, al menos, los objetivos o misión de la organización, el marco legal y regulatorio en el que se desarrollarán las actividades, los roles o funciones de seguridad, definiendo para cada uno, los deberes y responsabilidades de los cargos, así como el procedimiento para su designación y renovación, la estructura del comité o los comités para la gestión y coordinación de la seguridad, detallando su ámbito de responsabilidad, los miembros y la relación con otros elementos de la organización.

En este contexto, la Universidad de Málaga en su Reglamento de Administración Electrónica, realiza una firme apuesta por la seguridad como mecanismo para garantizar una Administración Electrónica que se desarrolle en un entono seguro y protegido frente a las amenazas recurrentes que suelen tener lugar en el ámbito de las TIC. Tanto es así, que en su artículo 8, enuncia la seguridad, junto a otros como calidad, accesibilidad, neutralidad, interoperabilidad o actualización de la información y los servicios, como uno de los principios a los que queda sujeta la Sede Electrónica de la Universidad de Málaga. Seguridad que, de conformidad con lo indicado en los párrafos que anteceden, se rige por lo dispuesto en el Esquema Nacional de Seguridad, según dispone el artículo 9.2. del Reglamento de Administración Electrónica de la Universidad de Málaga. De igual forma, el texto normativo al referirse a la gestión de la Sede Electrónica, en el artículo 13, atribuye de manera precisa la Administración Electrónica y el mantenimiento de dicha Sede, en particular, en lo referido a la implantación y actualización de las medidas de seguridad que garanticen la accesibilidad e integridad de la información y de los servicios que se ofrece en dicha Sede. Particular relevancia tiene el artículo 15 del Reglamento de Administración Electrónica de la Universidad de Málaga, dedicado a la "seguridad", en el que se insiste, literalmente, en que "La Sede Electrónica estará dotada de las medidas de seguridad que garanticen la confidencialidad, autenticidad e integridad de su contenido, así como el acceso permanente a ella", a la vez que atribuye al Consejo de Gobierno la aprobación de la política de seguridad de la información de la Universidad de Málaga. Si bien la seguridad es una constante a lo largo de todo el texto normativo, además, entre los órganos colegiados que el Reglamento establece para el asesoramiento y control del funcionamiento de la Administración Electrónica, fija, junto a otros, la Comisión de Seguridad de la Información y Protección de Datos de la Universidad de Málaga. Todo ello, enfatiza, más si cabe, en la necesidad de aprobar este Reglamento como norma que, inexorablemente en el marco y unida al Reglamento de Administración Electrónica, se centra en establecer el marco normativo de la política de seguridad de la Universidad de Málaga.

En virtud de todo lo cual, el Consejo de Gobierno de la Universidad de Málaga, en sesión celebrada el XX de XXXX de 2024, a propuesta del Consejo de Dirección, acuerda aprobar las siguientes normas:

TÍTULO I
DISPOSICIONES GENERALES

Artículo 1. Objeto y ámbito de aplicación.

El presente Reglamento de Política de Seguridad de la Información afecta a las diferentes actividades en las que participa la Universidad de Málaga a través de medios electrónicos, en concreto:

a) Las relaciones entre el estudiantado, el personal técnico, de gestión y de administración y servicios, el personal docente e investigador y la propia Universidad de Málaga.

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

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

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

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

Artículo 2. Marco normativo.

El marco normativo en materia de seguridad de la información viene conformado por:

- 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.
- Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos.
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Ley 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantías de los Derechos Digitales.
- 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.
- Reglamento X/2024, de XX de XX, de Administración Electrónica de la Universidad de Málaga.

Artículo 3. 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 en materia de

seguridad de la información establecidos en al artículo 5 del Esquema Nacional 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 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 pueda acceder a los activos de información, conozca sus responsabilidades, reduciendo así 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: 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 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 4. 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 responden a una jerarquía simple: el Comité de Seguridad de la Información y Protección de Datos da instrucciones a la persona responsable de la Seguridad de la Información que se encarga de cumplimentarla, supervisando que todos implementan las medidas de seguridad según lo establecido en la política de seguridad aprobada. Por su parte, la persona que ostente la delegación de Protección de Datos debe ser oído en todos los aspectos relacionados con la seguridad de los datos personales.

El Esquema Nacional de Seguridad establece cinco roles generales relacionados con su participación en la gestión y supervisión de la seguridad de la información:

- Comité de Seguridad de la Información
- Responsable de la Información.
- Responsable de los Servicios.
- Responsable de los Sistemas de Información.
- Responsable de Seguridad.

Artículo 5. Comité de Seguridad de la Información y Protección de Datos.

El Comité de Seguridad de la Información y Protección de Datos coordina la seguridad de la información y la protección de datos personales en la Universidad de Málaga. Estará compuesto por los siguientes miembros:

Presidente/a	Rector/a o persona en quien delegue
Secretario/a	Persona titular de la Secretaría General
Responsable de Información	Persona titular de la Secretaría General
Responsable de Servicio	Persona titular del Vicerrectorado con competencias en PDI
	Persona titular del Vicerrectorado con competencias en Estudiantes
	Persona titular del Vicerrectorado con competencias en PTGAS
Responsable de Seguridad	Persona Responsable de Seguridad
Responsable de Sistemas de Información	Persona titular de la Dirección de Tecnologías de la Información
Vocal	Persona titular de la Dirección del Gabinete Jurídico
Vocal	Persona titular de la Delegación del Rector/a para las Relaciones en el ámbito de la Salud
Delegado/a de Protección de Datos	Persona titular de la Delegación de Protección de Datos

A requerimiento del Comité de Seguridad de la Información y Protección de Datos se convocará a cualquier miembro de la comunidad universitaria, cuya intervención sea precisa.

Artículo 6. Funciones del Comité de Seguridad de la Información y Protección de Datos.

Corresponde al Comité de Seguridad de la Información y Protección de Datos, las siguientes funciones:

- Elaborar la estrategia de evolución de la Universidad de Málaga en lo que respecta a la seguridad de la información y a la protección de datos personales, fijando directrices y proponiendo la adopción de cuantas medidas se consideren convenientes en su ámbito de actuación.
- Atender las inquietudes que le sean trasladadas, tanto por los órganos de dirección como por los diferentes centros, departamentos o servicios de la Universidad de Málaga.
- Informar regularmente al Consejo de Dirección de la Universidad de Málaga.
- Informar a los empleados de los protocolos de actuación que se establezcan.
- Proponer a la Comisión de Formación, planes de formación específica en materias de su ámbito.
- 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 y de protección de datos.
- Resolver los conflictos de responsabilidad que en estas materias puedan aparecer entre los diferentes responsables y/o entre las diferentes áreas de la Universidad de Málaga, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.

Artículo 7. Presidencia y funciones.

1. El Comité de Seguridad de la Información y Protección de Datos estará presidido por el Rector/a o persona en quien delegue.

2. Son funciones del Comité de Seguridad de la Información y Protección de Datos, las siguientes:

a) Ostentar su representación.

b) Acordar la convocatoria de las sesiones ordinarias y extraordinarias y fijar su orden del día, teniendo en cuenta, en su caso, las peticiones de los demás integrantes de la Comisión.

c) Presidir las sesiones, moderar el desarrollo de los debates y suspenderlos por causas justificadas.

d) Asegurar el cumplimiento de la normativa vigente.

e) Ejercer cuantas otras funciones sean inherentes a su condición.

Artículo 8. Secretario/a y funciones.

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

- 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 9. Responsable de la Información y funciones.

1. Ejercerá como Responsable de la Información la persona que ostente la Secretaría General de la Universidad de Málaga, o persona en quien delegue.

2. Son funciones del Responsable de la Información de la Universidad de Málaga, las siguientes:

a) Velar por el buen uso y la protección de la información.

b) 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.

c) Adoptar las medidas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado.

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 10. Responsable del Servicio y funciones.

1. La figura del Responsable del Servicio recaerá en las personas que ocupen los Vicerrectorados con competencias en materia de Estudiantes, de PDI y del PTGAS de la Universidad de Málaga.

2. Son funciones y responsabilidades del Responsable del Servicio, las siguientes:

a) Tiene la responsabilidad última del uso que se haga de los servicios dirigidos al colectivo de su ámbito de competencias y, por tanto, de su protección.

b) Establecer los requisitos del servicio en materia de seguridad, incluyendo los requisitos de interoperabilidad, accesibilidad y disponibilidad.

c) Hacer cumplir adecuadamente la política, normativa y procedimientos de seguridad de los servicios.

Artículo 11. Responsable de Seguridad y funciones.

1. La figura del Responsable de Seguridad recaerá en la persona que ocupe la responsabilidad de la Unidad de Ciberseguridad de la Universidad de Málaga.

2. Son funciones y responsabilidades del Responsable de Seguridad, las siguientes:

a) Mantener la seguridad de la información y de los servicios prestados por los sistemas de información en su ámbito de responsabilidad, de acuerdo con lo establecido en la Política de Seguridad de la Universidad de Málaga.
b) Elaborar la Normativa Técnica de Seguridad de la Información, para su aprobación por el Comité de Seguridad de la Información y Protección de Datos.
c) Validar los procedimientos operativos de Seguridad de la Información.
d) Coordinar la realización de los análisis de riesgos, así como la efectiva implementación de los controles previstos para eliminar o reducir el riesgo.
e) Promover la formación y concienciación en materia de seguridad de la información.
f) Recopilar los requisitos de seguridad de los Responsables de Información y Servicio y determinar la categoría del Sistema.

Artículo 12. Responsable de Sistemas de Información y funciones.

1. La figura del Responsable de Sistemas de Información recaerá en la persona que ocupe la dirección de los servicios TIC de la Universidad de Málaga.

2. Son funciones y responsabilidades del Responsable de Sistemas de Información, las siguientes:

a) Asegurar el buen funcionamiento de los sistemas de información.
b) Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.
c) 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.
d) Definir la topología y sistema de gestión de los sistemas de información estableciendo los criterios de uso y los servicios disponibles en el mismo.
e) Asegurar que se elaboran procedimientos operativos de seguridad, planes de contingencia y emergencia.
f)

Artículo 13. Vocales y funciones.

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

a) Participar en las sesiones que se convoquen.
b) Contribuir con ideas y sugerencias para el buen desarrollo de las sesiones.

Capítulo II
Obligaciones y formación del personal

Artículo 14. Obligaciones del personal.

Los miembros de la Universidad de Málaga tienen la obligación de conocer esta Política de Seguridad, así como de conocer y cumplir toda la normativa que en la materia se establezca, siendo responsabilidad del Comité de Seguridad de la Información y Protección de Datos disponer los medios necesarios para que la información llegue a los afectados por esta normativa.

Artículo 15. Formación y concienciación.

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

Artículo 16. Cumplimiento de la Política.

La Política de Seguridad de la Información será de obligado cumplimiento para todo el personal que acceda a información que sea gestionada por la Universidad de Málaga, con independencia de cuál sea su destino, adscripción o relación con la misma.

Artículo 17. Terceras partes.

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

Disposición Adicional. Revisión de la Política de Seguridad de la Información.

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

Disposición Derogatoria Única.

Queda derogada la Política de Seguridad aprobada por el Consejo de Gobierno de la Universidad de Málaga el 28 de mayo de 2019, así como las demás disposiciones de la Universidad de Málaga que, siendo de igual o inferior rango, contradigan el presente el Reglamento.

Disposición Final. Entrada en vigor.

El presente Reglamento entrará en vigor al día siguiente de su publicación en el Boletín Oficial de la Universidad de Málaga.