POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

UNIVERSIDAD POLITÉCNICA DE MADRID

APROBADA EN LA SESION DEL CONSEJO DE GOBIERNO DE

18 DE DICIEMBRE DE 2025

VERSIÓN	FECHA CREACIÓN	AUTOR	APROBACIÓN
0.1	01/11/2025	Vicerrectorado para Universidad Digital	BORRADOR
0.2	02/12/2025	Vicerrectorado para Universidad Digital	BORRADOR
1.0	18/12/2025	Vicerrectorado para Universidad Digital	APROBADO EN CONSEJO DE GOBIERNO

Índice

1. Introducción

El Real Decreto 311/2022, de 3 de mayo por el que se regula el Esquema Nacional de Seguridad establece en su artículo 12.2 que "Cada administración pública contará con una política de seguridad formalmente aprobada por el órgano competente." Asimismo, ha de tenerse en cuenta el perfil de cumplimiento específico para universidades (CCN-STIC 881A de mayo de 2022).

La aprobación de esta Política de Seguridad de la Información (en adelante Política) pone de manifiesto el interés de la Universidad Politécnica de Madrid (en adelante UPM) en la gestión de la seguridad de la información. Con ella se establecen los objetivos y las responsabilidades necesarias para proteger los activos de información frente a daños accidentales o deliberados que puedan afectar a las dimensiones de seguridad de la información tratada o los servicios prestados. La UPM establecerá las medidas técnicas, organizativas y de control que garanticen la consecución de estos objetivos.

2. Misión de la Universidad Politécnica de Madrid

De conformidad con lo establecido en el Artículo 1 de sus Estatutos la UPM es una entidad de derecho público que goza de plena personalidad jurídica y patrimonio propio para el desarrollo de sus funciones y la consecución de sus fines, estando estos definidos en el Artículo 2 de los citados Estatutos.

La UPM, pone a disposición de la ciudadanía la realización de trámites online y nuevas vías de participación que garanticen el desarrollo y la eficacia de sus funciones y cometidos. Al potenciar el uso de las tecnologías de la información en la UPM se persigue fomentar la relación electrónica de todos los actores (docentes, estudiantes, investigadores, personal técnico de gestión y de administración y servicios y otros) con la universidad.

3. Declaración de la Política de Seguridad de la Información

Alcanzar algunos de los objetivos de la UPM depende de las Tecnologías de la Información y las Comunicaciones (en adelante TIC). Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la seguridad de la información tratada o los servicios prestados y estando siempre protegidos contra las amenazas o los incidentes con potencial para incidir en la confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad de la información tratada y los servicios prestados.

Para hacer frente a estas amenazas se requiere una estrategia que se adapte a los cambios en las condiciones del entorno de forma que se garantice la prestación continua de los servicios. Esto implica que se deben aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad (ENS), así como realizar un seguimiento continuo de los niveles de prestación de los

servicios, monitorizar y analizar las vulnerabilidades y preparar una respuesta efectiva a los ciberincidentes para garantizar la continuidad de los servicios prestados.

De este modo, todas las unidades administrativas de la universidad deben tener presente que la seguridad TIC es 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.

Por tanto, para la UPM, 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 para detectar cualquier incidente y reaccionando con agilidad a los incidentes para recuperar los servicios lo antes posible, según lo establecido en el Artículo 8 del ENS, con la aplicación de las medidas que se relacionan a continuación.

3.1 Prevención

La UPM debe evitar, o al menos prevenir en la medida que sea posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello implementa las medidas de seguridad determinadas por el ENS, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos. Estos controles, y los roles y responsabilidades de seguridad de todo el personal deben estar claramente definidos y documentados.

Para garantizar el cumplimiento de la Política, la UPM:

- Autoriza los sistemas antes de entrar en operación.
- Evalúa regularmente la seguridad, incluyendo análisis de los cambios de configuración realizados de forma rutinaria.
- Solicita la revisión periódica de los sistemas de información por parte de terceros con el fin de obtener una evaluación independiente.
- Establece los requisitos de seguridad que deben cumplir los servicios/suministros en los procesos de contratación.

3.2 Detección

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, es preciso monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia según lo establecido en el Artículo 10 del ENS (vigilancia continua y reevaluación periódica).

La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el Artículo 9 del ENS. Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables, tanto regularmente, como cuando se produzca una desviación significativa de los parámetros que se haya preestablecido como normales.

3.3 Respuesta

La UPM, establecerá las siguientes medidas:

- Mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar un punto de contacto para las comunicaciones con respecto a incidentes detectados en cada parte de la organización, así como en otros organismos.
- Establecer protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT, del inglés *Computer Emergency Response Team*).

3.4 Recuperación

Para garantizar la disponibilidad de los servicios críticos, la UPM dispone de planes de continuidad de los sistemas TIC como parte de su plan general de preservación del servicio y actividades de recuperación.

4. Principios básicos

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:

- Alcance estratégico: La seguridad de la información debe contar con el compromiso y apoyo de todos los niveles directivos de la universidad, de forma que pueda estar coordinada e integrada con el resto de las iniciativas estratégicas de la organización para conformar un todo coherente y eficaz.
- Diferenciación de responsabilidades: En los sistemas de información se diferenciará el responsable de la información, el responsable del servicio, el responsable de la seguridad y el responsable del sistema. La responsabilidad de la seguridad de los sistemas de información estará diferenciada de la responsabilidad sobre la explotación de los sistemas de información concernidos. En esta política de seguridad se detallarán las atribuciones de cada responsable y los mecanismos de coordinación y resolución de conflictos.
- Seguridad integral: La seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con los sistemas TIC. La seguridad de la información debe considerarse como parte de la operativa habitual, estando presente y aplicándose desde el diseño inicial de los sistemas TIC.
- 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.
- 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.

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

5. Objetivos de la Seguridad de la Información

La UPM establece como objetivos de la seguridad de la información los siguientes:

- Garantizar la calidad y protección de la información.
- Lograr la concienciación de los usuarios respecto a la seguridad de la información.
- Gestión de activos de información: Los activos de información de la universidad se encontrarán inventariados y categorizados y estarán asociados a un responsable.
- 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 su uso indebido, logrando la plena concienciación de los usuarios respecto a la seguridad de la información.
- 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.
- 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 TIC. 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.
- 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 de la organización.
- 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.
- Gestión de los incidentes de seguridad: Se implantarán los mecanismos apropiados para la correcta identificación, registro y resolución de los incidentes de seguridad.
- Garantizar la prestación continuada de los servicios: 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 con las necesidades de nivel de servicio de sus usuarios.

- Protección de datos: Se adoptarán las medidas técnicas y organizativas que corresponda implantar para atender los riesgos generados por su tratamiento para cumplir la legislación de seguridad y privacidad.
- 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.

6. Alcance

Esta Política se aplicará a los sistemas de información de la UPM relacionados con el ejercicio de sus competencias y a todos los usuarios con acceso autorizado a los mismos, sean o no empleados públicos y con independencia de la naturaleza de su relación jurídica con la universidad. Todos ellos tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y su Normativa de Seguridad derivada, siendo responsabilidad del Comité de Seguridad TIC disponer los medios necesarios para que la información llegue al personal afectado.

Quedarán fuera del alcance de esta Política aquellos ordenadores o dispositivos personales financiados a título individual, no inventariados a nombre de la Universidad, así como las acciones sobre ellos o riesgos de seguridad de tales elementos. No obstante, en el caso de que se acceda a la red o información corporativa mediante dichos ordenadores o dispositivos personales, quedarán sujetos a las obligaciones establecidas en la presente Política de Seguridad de la Información y a las normas e instrucciones de desarrollo.

7. Marco normativo

El marco normativo en que se desarrollan las actividades de la UPM y, en particular, la prestación de sus servicios electrónicos está integrado por las siguientes normas:

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS)
- Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad.
- Resolución de 7 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de Informe del Estado de la Seguridad.
- Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información.
- Resolución de 13 de abril de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad.

- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía 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 y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.
- Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público.
- Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.
- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual.
- Real Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto Básico del Empleado Público.
- Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la sociedad de la Información.
- Ley 19/2013, de 9 de diciembre, de Transparencia, Acceso a la Información Pública y Buen Gobierno.
- Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014.
- Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones.
- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza en la materia.
- 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 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.
- Ley Orgánica 2/2023, de 22 de marzo, del Sistema Universitario.
- Estatutos de la Universidad Politécnica de Madrid (Decreto 84/2025, de 22 de octubre, del Consejo de Gobierno, BOCM de 24 de octubre).

También forman parte del marco normativo las restantes normas aplicables a la Administración Electrónica de la UPM, comprendidas dentro del ámbito de aplicación de la presente Política, que se publicarán en la sede electrónica de la Universidad (https://sede.upm.es/)

8. Organización de la Seguridad

8.1 Comité de Seguridad TIC (COMSEGTIC): Funciones y Responsabilidades

El Comité de Seguridad TIC **coordina** la seguridad de la información en la UPM.

El Comité de Seguridad TIC reportará al Rector y estará formado por:

1. Miembros Permanentes:
   - Responsable de los Servicios: Vicerrector/a competente en materia de Tecnologías de la Información que actuará como presidente del COMSEGTIC.
   - Responsable de la Información: Secretario/a General, que actuará como secretario/a del COMSEGTIC.
   - Responsable de la Gerencia
   - Responsable de Seguridad: Responsable del Servicio de Seguridad TI, designado por el Rector.
   - Responsable del Sistema: Dirección de los Servicios Informáticos
   - Responsable de los Servicios Jurídicos.
   - Un representante de los directores de Centro elegido entre ellos
   - Un representante de los Institutos y Centros de Investigación elegido entre ellos.
   - Delegado de Protección de Datos: Participará con voz, pero sin voto en las reuniones del COMSEGTIC de seguridad de la información cuando en el mismo 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 la opinión del Delegado de Protección de Datos.

2. Miembros Invitados:
   - El COMSEGTIC podrá contar con asesores que se consideren oportunos para los temas en cuestión, pudiendo incluso acudir un representante del Centro Criptológico Nacional (CCN), con voz, pero sin voto.
   - El COMSEGTIC podrá invocar la presencia en sus reuniones tanto de otros representantes de la universidad como de especialistas externos, de los sectores público, privado y/o académico, cuya presencia, por razón de su experiencia o vinculación con los asuntos tratados, sea necesaria o aconsejable. Estos invitados tendrán voz, pero no tendrán voto.

Las responsabilidades anteriores vendrán determinadas por el desempeño de los cargos o destinos, estatutarios o no, a los que se atribuyen. En caso de ausencia, vacante o impedimento, el Rector designará provisionalmente la persona que desempeñará dicha tarea.

El COMSEGTIC se reunirá, al menos dos veces al año, sin perjuicio de que, en atención a las necesidades derivadas del cumplimiento de sus fines y atribuciones requiera de una mayor frecuencia en las reuniones.

Las reuniones se convocarán por su Presidencia, a través del Secretario/a, a su iniciativa o por mayoría de sus miembros natos.

Las decisiones se adoptarán por mayoría simple de los miembros permanentes, decidiendo en caso de empate el voto de calidad otorgado al presidente.

El COMSEGTIC tendrá las siguientes funciones:

1. Estar informado de la normativa que regula la Certificación de Conformidad con el ENS, incluyendo sus normas de acreditación, certificación, guías, manuales, procedimientos e instrucciones técnicas.
2. Estar informado de la relación de Entidades de Certificación acreditadas y organizaciones, públicas y privadas, certificadas.
3. Estar informado de la relación de esquemas de certificación de la seguridad con los que la Administración Pública tiene establecidos arreglos o acuerdos de reconocimiento mutuo de certificados.
4. Proponer directrices y recomendaciones, que serán recogidas en las correspondientes actas de las reuniones del COMSEGTIC, a las que su presidente, deberá dar cumplida respuesta.
5. Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información, para asegurar que estos sean consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades.
6. Atender las inquietudes, en materia de Seguridad de la Información, de la Administración y de las diferentes áreas, informando regularmente del estado de la seguridad de la información a la Dirección.
7. Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables y/o entre diferentes Departamentos, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.
8. Asesorar en materia de seguridad de la información, siempre y cuando le sea requerido.
9. Revisar y proponer la Política de Seguridad de la Información al Consejo de Gobierno de la Universidad.
10. Aprobar la Normativa de Uso de Medios electrónicos para todo el personal.
11. Aprobar el Mapa de Normativa con la lista de Normativa y Procedimientos de seguridad para la implantación del ENS.
12. Promover la mejora continua del Sistema de Gestión de la Seguridad de la Información.
13. Elaborar la estrategia de evolución de la UPM en lo que respecta a seguridad de la información.
14. Informar regularmente del estado de la seguridad de la información al Rector de la UPM.

8.2 Roles: Funciones y Responsabilidades

Las funciones y responsabilidades de los miembros del COMSEGTIC están definidas para garantizar la necesaria independencia y la ausencia de conflictos de intereses.

A efectos de velar por la seguridad de la información en la UPM, se definen las siguientes figuras de las que se detallan sus funciones y responsabilidades:

Responsable de la Información y de los Servicios

Serán funciones de los Responsables de la Información y de los Servicios:

1. Establecer y elevar para su aprobación al COMSEGTIC los requisitos de seguridad aplicables a la Información (niveles de seguridad de la Información) y a los Servicios (niveles de seguridad de los servicios), dentro del marco establecido en el Anexo I del RD ENS, pudiendo recabar una propuesta al Responsable de Seguridad y teniendo en cuenta la opinión del Responsable del Sistema.
2. Dictaminar respecto a los derechos de acceso a la información y los servicios.
3. Aceptar los niveles de riesgo residual que afectan a la información y los servicios.
4. Poner en comunicación del Responsable de Seguridad cualquier variación respecto a la Información y los Servicios de los que es responsable, especialmente la incorporación de nuevos Servicios o Información a su cargo. El cual dará traslado de dichos cambios, al COMSEGTIC, en su próxima reunión.

Dado que el/la responsable de la información actúa como secretario/a del COMSEGTIC, sus funciones se ven incrementadas con las propias del secretario/a:

1. Convocar las reuniones del COMSEGTIC, a petición de su Presidencia.
2. Preparar los temas a tratar en las reuniones del COMSEGTIC, aportando información puntual para la toma de decisiones.
3. Elaborar el acta de las reuniones.
4. Ser el responsable de la ejecución directa o delegada de las decisiones del COMSEGTIC.
5. Invitar de forma consultiva a las reuniones a cualquier persona que el COMSEGTIC considere conveniente para el desarrollo de sus funciones.

Responsable de la Seguridad

Serán funciones del Responsable de Seguridad:

1. Mantener y verificar el nivel adecuado de seguridad de la Información manejada y de los Servicios electrónicos prestados por los sistemas de información.
2. Promover la formación y concienciación en materia de seguridad de la información.
3. Gestionar los incidentes de seguridad y notificar en su caso a los organismos competentes (CERT) en el ámbito de ciberseguridad.
4. Designar responsables de la ejecución del análisis de riesgos, de la Declaración de Aplicabilidad. Identificar medidas de seguridad y determinar las configuraciones necesarias.
5. Proporcionar asesoramiento para la determinación de la Categoría del Sistema, en colaboración con el Responsable del Sistema y/o COMSEGTIC
6. Participar en la elaboración e implantación de los planes de mejora de la seguridad y, llegado el caso, en los planes de continuidad, procediendo a su validación.
7. Gestionar las revisiones externas o internas del sistema.

8. Gestionar los procesos de certificación.
9. Elevar al COMSEGTIC la aprobación de cambios y otros requisitos del sistema.
10. Aprobar los procedimientos de seguridad de su competencia que forman parte del Mapa Normativo y poner en conocimiento del COMSEGTIC de las modificaciones que se hayan realizado a lo largo del periodo en curso.

El Responsable de la Seguridad corresponderá a un cargo o funcionario, de nivel ejecutivo, designado formalmente por el Rector o el Equipo de Dirección. El Responsable de Seguridad no podrá ser un órgano de gobierno unipersonal de la Universidad.

Responsable del Sistema

Serán funciones del Responsable del Sistema:

1. Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida, elaborando los procedimientos operativos necesarios.
2. Definir la topología y la gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo.
3. Detener el acceso a información o prestación de servicio si tiene el conocimiento de que estos presentan deficiencias graves de seguridad.
4. Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.
5. Proporcionar asesoramiento para la determinación de la Categoría del Sistema, en colaboración con el Responsable de Seguridad y/o COMSEGTIC.
6. Participar en la elaboración e implantación de los planes de mejora de la seguridad y llegado el caso en los planes de continuidad.
7. Llevar a cabo, en su caso, las funciones del administrador de la seguridad del sistema:
   - La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad.
   - La gestión de las autorizaciones concedidas a los usuarios del sistema, en particular los privilegios concedidos, incluyendo la monitorización de la actividad desarrollada en el sistema y su correspondencia con lo autorizado.
   - Aprobar los cambios en la configuración vigente del Sistema de Información.
   - Asegurar que los controles de seguridad establecidos son cumplidos estrictamente.
   - Asegurar que son aplicados los procedimientos aprobados para manejar el 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.
   - Monitorizar el estado de seguridad proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica.
   - Informar al Responsable de Seguridad 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.

De forma directa o en colaboración con la Oficina de Seguridad TIC el Responsable del Sistema asumirá también las siguientes funciones:

- Vigilar y monitorizar la seguridad de los sistemas, y de los dispositivos de defensa, ya sea mediante interfaces previstas o instalando las correspondientes sondas.
- Análisis y correlación de eventos de seguridad y registros de actividad de los sistemas.
- Operaciones de seguridad sobre los dispositivos de defensa.
- Podrá constituir un Equipo de Respuesta a Incidentes de Seguridad: Realizar un seguimiento de la gestión de los incidentes de seguridad y recomendar posibles actuaciones respecto de ellos.
- Servicio de Alerta Temprana (SAT) de alertas de seguridad en las redes corporativas y en las conexiones a Internet de los sistemas.
- Gestión de vulnerabilidades (análisis y determinación de las acciones de subsanación/parcheado) de aplicaciones y servicios.
- Análisis forense digital y de seguridad.
- Servicio de cibervigilancia que posibilite la prospectiva sobre la ciberamenaza.

Cuando la complejidad del sistema lo justifique, el Responsable del Sistema podrá designar los responsables de sistema delegados que considere necesarios, que tendrán dependencia funcional directa de aquél y serán responsables en su ámbito de todas aquellas acciones que les delegue el mismo. De igual modo, también podrá delegar en otro/s funciones concretas de las responsabilidades que se le atribuyen.

Administradores de la Seguridad del Sistema

1. Implementar, gestionar y mantener las medidas de seguridad aplicables al Sistema de Información.
2. Gestionar, configurar y actualizar, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad del Sistema de Información.
3. Gestionar las autorizaciones concedidas a los usuarios del sistema, en particular los privilegios concedidos, incluyendo el desarrollo de la actividad conforme a lo autorizado.
4. Asegurar la aplicación de los procedimientos y medidas de seguridad aprobados para manejar el sistema de información.
5. 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.
6. 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.
7. Informar a los Responsables de la Seguridad y del Sistema de cualquier anomalía, disfunción, compromiso o vulnerabilidad relacionada con la seguridad.
8. Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución.

El COMSEGTIC podrá nombrar cuantos Administradores de la Seguridad considere necesarios a propuesta del Responsable del Sistema o del Responsable de Seguridad. El Administrador de Seguridad dependerá del Responsable que haya propuesto su nombramiento.

Delegado de protección de datos

Serán funciones del Delegado de Protección de Datos:

- Informar y asesorar a la UPM y a los usuarios que se ocupen del tratamiento, de las obligaciones que les incumben en virtud de la normativa vigente en materia de Protección de Datos.
- Supervisar el cumplimiento de lo dispuesto en normativa de seguridad y de las políticas internas de la UPM, en materia de protección de datos, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes.
- Ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisará su aplicación.
- Cooperar con la Agencia Española de Protección de Datos cuando ésta lo requiera, actuando como punto de contacto con ésta para cuestiones relativas al tratamiento de datos.
- El Delegado de Protección de datos desempeñará sus funciones prestando atención a los riesgos asociados a las operaciones de tratamiento. Para ello debe ser capaz de:
    - Recabar información para determinar las actividades de tratamiento.
    - Analizar y comprobar la conformidad de las actividades de tratamiento.
    - Informar, asesorar y emitir recomendaciones al responsable o el encargado del tratamiento.
    - Recabar información para supervisar el registro de las operaciones de tratamiento.
    - Asesorar en el principio de la protección de datos por diseño y por defecto. o Asesorar sobre si se lleva a cabo o no las evaluaciones de impacto, metodología, salvaguardas a aplicar, etc.
    - Priorizar actividades en base a los riesgos. o Asesorar al Responsable de Tratamiento sobre áreas a cometer a auditorías, actividades de formación a realizar y operaciones de tratamiento a dedicar más tiempo y recursos.

8.3 Oficina de Seguridad TIC

Dentro de la estructura de gobernanza de la ciberseguridad se constituye la Oficina de Seguridad TIC, cuyas competencias estarán relacionadas con las siguientes áreas de trabajo: adecuación al ENS, normativa y gestión de riesgos, análisis y mejora continua, seguridad en las interconexiones y conectividad y otras funciones conexas o concordantes.

Estará compuesto por:

- El Director de la Oficina de seguridad TIC, que será el Responsable de Seguridad (o persona en quien delegue) y que actuará como enlace con el COMSEGTIC.

- Todos aquellos administradores de seguridad que el Responsable de Seguridad determine que sean necesarios

Las funciones de la Oficina de Seguridad TIC serán, entre otras que les puedan ser encomendadas por COMSEGTIC:

a) Gestión y operativa de la seguridad del Proyecto de Adecuación, Implantación y gestión de la Conformidad en el ENS, análisis y gestión de riesgos, explotación, normativa y mantenimiento.
b) Redacción y presentación de propuestas al COMSEGTIC. Elaborará los aspectos relacionados con la ciberseguridad y los debatirá en primera instancia, para ser trasladados al COMSEGTIC.
c) Promover de la mejora continua del sistema de gestión de la Seguridad de la Información. Para ello se encargará de:
    - Elaborar (y revisar regularmente) la Política de Seguridad de la Información para su traslado al COMSEGTIC para su revisión y posterior aprobación del órgano superior.
    - Elaborar la normativa de Seguridad de la Información para su aprobación por el Responsable de Seguridad, con conocimiento del COMSEGTIC.
    - Verificar los procedimientos de seguridad de la información y demás documentación para su aprobación.
    - Elaborar programas de formación destinados a formar y sensibilizar al personal en materia de seguridad de la información y protección de datos.
    - Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios desde el punto de vista de seguridad de la información. o Proponer planes de mejora de la seguridad de la información, con su dotación presupuestaria correspondiente, priorizando las actuaciones en materia de seguridad cuando los recursos sean limitados.
    - Realizar un seguimiento de los principales riesgos residuales asumidos y recomendar posibles actuaciones respecto de ellos.
    - Promover la realización de las auditorías periódicas ENS y RGPD que permitan verificar el cumplimiento de las obligaciones de la universidad en materia de seguridad de la Información y protección de datos.

8.4 Resolución de conflictos

En caso de conflicto entre los diferentes responsables y/o entre diferentes servicios de la institución, éste será resuelto por el superior jerárquico de los mismos. En defecto de lo anterior, prevalecerá la decisión del COMSEGTIC, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.

9. Desarrollo de la Política de Seguridad de la Información.

La UPM establece un marco de normas en materia de seguridad de la información estructurado en diferentes niveles de forma que los objetivos marcados por el presente documento tengan un desarrollo específico:

- Primer nivel: la Política de Seguridad de la Información y la Normativa de uso de los recursos TIC. Corresponde al Consejo de Gobierno de la UPM su aprobación.
- Segundo nivel: Las normativas de seguridad, constituido por las normas de seguridad derivadas de las anteriores y que definen qué hay que proteger y los requisitos de seguridad deseados. Establecen un conjunto de expectativas y requisitos que deben ser alcanzados para poder satisfacer y cumplir cada uno de los objetivos de seguridad establecidos en la Política. El COMSEGTIC será responsable de la aprobación y difusión de estas normativas.
- Tercer nivel: los procedimientos de seguridad de la información. Conjunto de documentos que describen explícitamente y paso a paso cómo realizar una cierta actividad.
- Cuarto nivel: documentación de buenas prácticas, recomendaciones, guías, cursos de formación, presentaciones, etc.

El Responsable de seguridad será el encargado de la elaboración y difusión de los documentos de tercer y cuarto nivel.

Todos los documentos deberán estar a disposición de todos los miembros de la UPM que necesiten conocerlas, en particular para el personal que utilice, haga funcionar o administre los sistemas de información y comunicaciones.

Las normativas de seguridad deberán estar disponibles en la intranet corporativa.

El COMSEGTIC establecerá en cada caso las limitaciones al acceso, uso y reutilización para el usuario o receptor de estos documentos.

La revisión de cada documento y la propuesta de nuevas versiones realizada por cualquiera de las áreas afectadas o por los órganos de la Universidad se notificarán al Responsable de Seguridad, que canalizará las propuestas a través del COMSEGTIC. Las nuevas versiones de cualquiera de estos documentos se deberán comunicar, a su ámbito de uso y el nivel de difusión que requieran, para que el personal afectado pueda eliminar las versiones obsoletas.

10. Datos de Carácter Personal

La UPM, solo recogerá y tratará datos personales cuando sean adecuados, pertinentes y no excesivos y éstos se encuentren en relación con el ámbito y las finalidades para las que se hayan obtenido. De igual modo, adoptará las medidas de índole técnica y organizativas necesarias para el cumplimiento de la normativa de Protección de Datos.

11. Gestión de Riesgos

Todos los sistemas afectados por esta Política están sujetos a un análisis de riesgos con el objetivo de evaluar las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá:

- Regularmente, al menos de forma anual.
- Cuando se produzcan cambios en la información y/o los servicios manejados de manera significativa.

- Cuando ocurra un incidente grave de seguridad o se detecten vulnerabilidades graves.

El Responsable de la Seguridad será el encargado de que se realice el análisis de riesgos, así como de identificar carencias y debilidades y ponerlas en conocimiento del COMSEGTIC.

El COMSEGTIC dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

El proceso de gestión de riesgos comprenderá las siguientes fases:

- Categorización de los sistemas.
- Análisis de riesgos.
- El COMSEGTIC procederá a la selección de medidas de seguridad a aplicar que deberán de ser proporcionales a los riesgos y estar justificadas.

Las fases de este proceso se realizarán según lo dispuesto en los Anexos I y II del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS) ,, y siguiendo las normas, instrucciones, Guías CCN-STIC y recomendaciones para la aplicación de este elaboradas por el Centro Criptológico Nacional.

En particular, para realizar el análisis de riesgos, como norma general se utilizará una metodología reconocida de análisis y gestión de riesgos.

12. Obligaciones de los miembros de la Comunidad Universitaria

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

Todos los miembros de la UPM tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y las normativas que se deriven, siendo responsabilidad del COMSEGTIC disponer los medios necesarios para que la información llegue a los afectados. Cuando un miembro de la UPM sea requerido como participante en este programa su participación será obligatoria.

Los miembros de la UPM recibirán formación en seguridad de la información. Se establecerá un programa continuo de concienciación para atender a todos los miembros de la comunidad universitaria, en particular a los de nueva incorporación.

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.

El COMSEGTIC podrá apreciar si por parte del personal del personal de la UPM en el ejercicio de sus actividades profesionales, existe algún tipo de incumplimiento en las obligaciones previstas en la Política de Seguridad de la Información o en su normativa e instrucciones de desarrollo.

El incumplimiento de las obligaciones y medidas de seguridad establecidas en el presente documento conllevará la aplicación de la normativa en materia disciplinaria vigente en cada momento.

En el caso de detectarse incumplimiento de las medidas contempladas en esta Política de Seguridad o en sus normativas de desarrollo, se podrán aplicar medidas preventivas y correctoras, encaminadas a proteger los sistemas TIC, sin perjuicio de la correspondiente exigencia de responsabilidad disciplinaria o el ejercicio por parte de la UPM de las acciones oportunas previstas en la legislación vigente.

13. Terceras partes

Cuando la UPM preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipes de esta Política de Seguridad de la Información, se establecerán canales para reporte y coordinación de los respectivos Comités o Comisiones de Seguridad de la Información y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad. El responsable de seguridad de la información actuará como persona de contacto para la seguridad de los servicios e información tratada.

Cuando la UPM utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad de la Información y de la normativa de seguridad que ataña a dichos servicios o información. Dicha tercera parte tendrá obligación de designar una persona de contacto en materia de seguridad, y 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 está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política.

Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte según se indica 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 los responsables de la información y los servicios afectados antes de seguir adelante.

La obligación de comunicar la Política de Seguridad de la Información a terceras partes recae en los responsables de los proyectos de investigación, las unidades gestoras de contratos públicos, unidades proponentes de convenios o unidades promotoras de cualquier otro tipo de colaboraciones que afecten a la seguridad de la información.

14. Notificación de incidentes

De conformidad con lo dispuesto en el artículo 33 del ENS, la UPM notificará al CCN aquellos incidentes que tengan un impacto significativo en la seguridad de la información manejada y en los servicios prestados, en relación con la categorización de sistemas recogida en el Anexo I de dicho cuerpo legal o de acuerdo con la correspondiente Instrucción Técnica de Seguridad.

15. Mejora continua

La gestión de la seguridad de la información es un proceso sujeto a permanente actualización. Los cambios en la organización, las amenazas, las tecnologías y/o la legislación son un ejemplo en los que es necesaria una mejora continua de los sistemas. Por ello, es necesario implantar un proceso permanente que comportará, entre otras acciones:

a) Revisión de la Política de Seguridad de la Información.
b) Revisión de los servicios e información y su categorización.
c) Ejecución con periodicidad anual del análisis de riesgos.
d) Realización de auditorías internas o, cuando procedan, externas.
e) Revisión de las medidas de seguridad.
f) Revisión y actualización de las normas y procedimientos.

16. Modificaciones

Versión	Fecha	Modificaciones respecto a la versión anterior
1	18 de diciembre de 2025	Ninguna

17. Aprobación y entrada en vigor

Texto aprobado el día 18 de diciembre de 2025 por acuerdo del Consejo de Gobierno de la Universidad Politécnica de Madrid.

Esta Política de Seguridad de la Información será efectiva desde su fecha de aprobación y hasta que sea reemplazada por una nueva Política.

Clausula Residual

Asimismo, se deberán tener en cuenta las posibles modificaciones normativas y avances técnicos que puedan afectar al alcance de la presente Política de Seguridad de la Información.