



Documentos

UCM Serie:

Seguridad

SE0001 Política de Seguridad de la Información


Versión del Documento 2.0

14-02-2022

El contenido de este documento es propiedad de la Universidad Complutense. La información aquí contenida sólo debe ser utilizada para el fin para el que es suministrada, y este documento y todas sus copias deben ser devueltos a la Universidad si así se solicita.

Centro de Proceso de Datos
Av. Complutense. s/n. 28040 Madrid.

Código Seguro De Verificación	6339-5553-6D6BP3035-7477	Estado	Fecha y hora
Firmado Por	Jorge Jesus Gomez Sanz - Vicerrector de Tecnología y Sostenibilidad de la Universidad Complutense de Madrid Vice-Rector Of Technology And Sustainability Of The Universidad Complutense de Madrid	Firmado	06/04/2022 11:20:22
Observaciones		Página	1/18
Uri De Verificación	https://sede.ucm.es/verificacion?csv=6339-5553-6D6BP3035-7477		
Normativa	Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015).		





SE0001	Versión	Pág.
Política de Seguridad de la Información	2.0	2 de 18

INDICE

1	INTRODUCCIÓN	3
2	ALCANCE Y ÁMBITO DE APLICACIÓN	4
3	DEFINICIONES, ACRÓNIMOS Y ABREVIATURAS	5
4	REFERENCIAS.....	6
5	IMPORTANCIA DE LA SEGURIDAD DE LA INFORMACIÓN	7
6	PRINCIPIOS BÁSICOS.....	8
7	OBJETIVOS EN SEGURIDAD	10
8	ORGANIZACIÓN	11
9	ESTRUCTURACIÓN DE LA DOCUMENTACIÓN DE SEGURIDAD	12
10	REVISIÓN Y APROBACIÓN.....	14
11	ANEXO I. REQUISITOS DE SEGURIDAD DE OBLIGADO CUMPLIMIENTO.....	16
	1.1 LA SEGURIDAD EN LA ORGANIZACIÓN	16
	1.2 ANÁLISIS Y GESTIÓN DE RIESGOS.....	16
	1.3 GESTIÓN DE PERSONAL	16
	1.4 PROFESIONALIDAD	16
	1.5 AUTORIZACIÓN Y CONTROL DE ACCESO	17
	1.6 PROTECCIÓN DE LAS INSTALACIONES.....	17
	1.7 ADQUISICIÓN DE PRODUCTOS.....	17
	1.8 SEGURIDAD POR DEFECTO	17
	1.9 INTEGRIDAD Y ACTUALIZACIÓN DEL SISTEMA.....	17
	1.10 PROTECCIÓN DE LA INFORMACIÓN ALMACENADA Y EN TRÁNSITO	18
	1.11 PREVENCIÓN ANTE OTROS SISTEMAS DE INFORMACIÓN INTERCONECTADOS	18
	1.12 REGISTRO DE ACTIVIDAD.....	18
	1.13 GESTIÓN DE INCIDENTES DE SEGURIDAD	18
	1.14 CONTINUIDAD DE LA ACTIVIDAD	18
	1.15 GESTIÓN DE LA SEGURIDAD Y MEJORA CONTINUA.....	18

Centro de Proceso de Datos
Av. Complutense. s/n. 28040 Madrid.

Código Seguro De Verificación	6339-5553-6D6BP3035-7477	Estado	Fecha y hora
Firmado Por	Jorge Jesus Gomez Sanz - Vicerrector de Tecnología y Sostenibilidad de la Universidad Complutense de Madrid Vice-Rector Of Technology And Sustainability Of The Universidad Complutense de Madrid	Firmado	06/04/2022 11:20:22
Observaciones		Página	2/18
Uri De Verificación	https://sede.ucm.es/verificacion?csv=6339-5553-6D6BP3035-7477		
Normativa	Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015).		





SE0001	Versión	Pág.
Política de Seguridad de la Información	2.0	3 de 18

1 INTRODUCCIÓN

Este documento constituye la Política de Seguridad de la Información de la Universidad Complutense de Madrid (en adelante UCM), en cumplimiento del artículo 11 del Real Decreto 3/2010 de 8 de enero, por el que se regula los requisitos mínimos de Seguridad en el ámbito de la Administración Electrónica, y de la medida de seguridad org.1 contemplada en el Anexo II de dicho Real Decreto.

En este sentido, el mencionado 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.”*

La estructura de este documento sigue las pautas establecidas por las guías del Centro Criptológico Nacional, para la redacción de la Política de Seguridad de la Información en el ámbito del Esquema Nacional de Seguridad.

La Política de Seguridad de la Información recoge la postura de UCM en cuanto a la seguridad de la información y establece los criterios de obligado cumplimiento que deben regir la actividad del organismo en cuanto a la seguridad, tal como se describe en el anexo I de este documento.


El objetivo de la Seguridad de la Información es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.

Los sistemas de información deben estar protegidos contra amenazas con potencial para incidir en la disponibilidad, integridad, confidencialidad, autenticidad, trazabilidad, 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.

Esto implica que se deben aplicar las medidas de seguridad exigidas por el Esquema Nacional de Seguridad (ENS), el Reglamento General de Protección de Datos (RGPD) y la Ley de Protección de Datos y Garantía de los Derechos Digitales (LOPDgdd), 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.

Centro de Proceso de Datos
Av. Complutense. s/n. 28040 Madrid.

Código Seguro De Verificación	6339-5553-6D6BP3035-7477	Estado	Fecha y hora
Firmado Por	Jorge Jesus Gomez Sanz - Vicerrector de Tecnología y Sostenibilidad de la Universidad Complutense de Madrid Vice-Rector Of Technology And Sustainability Of The Universidad Complutense de Madrid	Firmado	06/04/2022 11:20:22
Observaciones		Página	3/18
Uri De Verificación	https://sede.ucm.es/verificacion?csv=6339-5553-6D6BP3035-7477		
Normativa	Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015).		





SE0001	Versión	Pág.
Política de Seguridad de la Información	2.0	4 de 18

2 ALCANCE Y ÁMBITO DE APLICACIÓN

Para responder a su misión de ofrecer a la comunidad universitaria servicios adecuados, protegidos de la destrucción, indisponibilidad, manipulación o revelación no autorizada de la información, la UCM reconoce expresamente la importancia de diseñar e implementar controles de seguridad para asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad, y conservación de los datos, informaciones y servicios utilizados que se gestionen en el ejercicio de sus competencias.

La presente Política pretende describir y formalizar la posición y las directrices principales de la seguridad de la información.

Esta Política debe ser conocida y cumplida por todo el personal de UCM, independientemente del puesto, cargo y responsabilidad dentro del mismo.

Todas las personas que intervengan en cualquier fase del tratamiento de datos están sujetas al deber de confidencialidad al que se refiere el artículo 5.1.f) del RGPD y 5 de la LOPDgdd, y podrán responder del tratamiento que se realice sobre los datos que manejen.

Centro de Proceso de Datos
Av. Complutense. s/n. 28040 Madrid.

Código Seguro De Verificación	6339-5553-6D6BP3035-7477	Estado	Fecha y hora
Firmado Por	Jorge Jesus Gomez Sanz - Vicerrector de Tecnología y Sostenibilidad de la Universidad Complutense de Madrid Vice-Rector Of Technology And Sustainability Of The Universidad Complutense de Madrid	Firmado	06/04/2022 11:20:22
Observaciones		Página	4/18
Uri De Verificación	https://sede.ucm.es/verificacion?csv=6339-5553-6D6BP3035-7477		
Normativa	Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015).		






SE0001	Versión	Pág.
Política de Seguridad de la Información	2.0	5 de 18

3 DEFINICIONES, ACRÓNIMOS Y ABREVIATURAS

UCM	Universidad Complutense de Madrid
ENS	Esquema Nacional de Seguridad
RGPD	Reglamento General de Protección de datos
LOPDgdd	Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales

Centro de Proceso de Datos
Av. Complutense. s/n. 28040 Madrid.

Código Seguro De Verificación	6339-5553-6D6BP3035-7477	Estado	Fecha y hora	
Firmado Por	Jorge Jesus Gomez Sanz - Vicerrector de Tecnología y Sostenibilidad de la Universidad Complutense de Madrid Vice-Rector Of Technology And Sustainability Of The Universidad Complutense de Madrid	Firmado	06/04/2022 11:20:22	
Observaciones		Página	5/18	
Uri De Verificación	https://sede.ucm.es/verificacion?csv=6339-5553-6D6BP3035-7477			
Normativa	Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015).			



SE0001	Versión	Pág.
Política de Seguridad de la Información	2.0	6 de 18

4 REFERENCIAS

- 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 Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.
- Ley Orgánica 6/2001, de 21 de diciembre, de Universidades.
- Ley Orgánica 4/2007, de 12 de abril, por la que se modifica la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades (Disposición adicional vigésima primera - Protección de datos de carácter personal).
- Estatutos de la Universidad Complutense de Madrid, aprobados por Decreto 32/2017, de 21 de marzo, del Consejo de Gobierno de la Comunidad de Madrid, parcialmente modificados por Decreto 5/2018, de 23 de enero.
- 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.
- Real Decreto 3/2010 del 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, modificado por Real Decreto 951/2015, de 23 de octubre.
- 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.
- Catálogo de servicios de informática de la UCM aprobado por Consejo de Gobierno el 30 de enero de 2003.
- UNE 66925:2002 IN. Directrices para la documentación de sistemas de gestión de la calidad.
- Acuerdo del Consejo de Gobierno de fecha 27 de mayo de 2014, por el que se aprueba el Reglamento de Creación del Comité de Seguridad de la Información de la Universidad Complutense de Madrid (BOUC nº11, 12 de junio de 2014).
- SE0002 Organización de la Seguridad de la Información.
- DTI-USPI-doc-Metodología de Análisis y Gestión de Riesgos

GUIAS DE REFERENCIAS

- CCN-STIC-801: ENS - Responsabilidades y funciones.
- CCN-STIC-805: ENS - Política de Seguridad de la Información.

Centro de Proceso de Datos
Av. Complutense. s/n. 28040 Madrid.

Código Seguro De Verificación	6339-5553-6D6BP3035-7477	Estado	Fecha y hora
Firmado Por	Jorge Jesus Gomez Sanz - Vicerrector de Tecnología y Sostenibilidad de la Universidad Complutense de Madrid Vice-Rector Of Technology And Sustainability Of The Universidad Complutense de Madrid	Firmado	06/04/2022 11:20:22
Observaciones		Página	6/18
Uri De Verificación	https://sede.ucm.es/verificacion?csv=6339-5553-6D6BP3035-7477		
Normativa	Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015).		





SE0001	Versión	Pág.
Política de Seguridad de la Información	2.0	7 de 18

5 IMPORTANCIA DE LA SEGURIDAD DE LA INFORMACIÓN

La consagración del derecho de los ciudadanos a relacionarse con la Administración por medios electrónicos implica la necesidad de facilitar el ejercicio de este derecho en condiciones de igualdad y libertad.

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

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

La UCM, en cumplimiento de la Disposición adicional primera de Ley Orgánica 3/2018, de 05 de diciembre, de Protección de Datos y Garantía de los Derechos Digitales, deberá aplicar a los tratamientos de datos personales las medidas de seguridad que correspondan de las previstas en el Esquema Nacional de Seguridad.

Con objeto de alcanzar las garantías que exigen dichas normativas en el ámbito de la Universidad Complutense de Madrid (UCM), se crea el Comité de Seguridad de la Información, que tiene como misión principal establecer un plan de adecuación de los Sistemas de Información al ENS y las medidas de seguridad aplicables a los tratamientos de datos de carácter personal, de manera que se aborde la seguridad como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos relacionados con el Sistema, tal y como establece el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica; además en este marco normativo la política de seguridad debe identificar unos claros responsables para velar por su cumplimiento y hacer que sea conocida por todos los miembros de la organización.

Centro de Proceso de Datos
Av. Complutense. s/n. 28040 Madrid.

Código Seguro De Verificación	6339-5553-6D6BP3035-7477	Estado	Fecha y hora
Firmado Por	Jorge Jesus Gomez Sanz - Vicerrector de Tecnología y Sostenibilidad de la Universidad Complutense de Madrid Vice-Rector Of Technology And Sustainability Of The Universidad Complutense de Madrid	Firmado	06/04/2022 11:20:22
Observaciones		Página	7/18
Uri De Verificación	https://sede.ucm.es/verificacion?csv=6339-5553-6D6BP3035-7477		
Normativa	Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015).		





SE0001	Versión	Pág.
Política de Seguridad de la Información	2.0	8 de 18

6 PRINCIPIOS BÁSICOS

Para poder acometer con éxito los objetivos de seguridad se deben definir y asignar responsabilidades y competencias en seguridad de la información. En las decisiones en materia de seguridad deberán tenerse en cuenta los siguientes principios básicos:

- La seguridad se entenderá como un **proceso integral** constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con los servicios prestados. Por lo tanto, se excluye cualquier actuación puntual o tratamiento coyuntural.

Se prestará la máxima atención a la concienciación de las personas que intervienen en el proceso y a sus responsables jerárquicos, para que, ni la ignorancia, ni la falta de organización y coordinación, ni instrucciones inadecuadas, sean fuentes de riesgo para la seguridad.

- El **análisis y gestión de riesgos** permanentemente actualizados son una parte esencial del proceso de seguridad, que requerirá la implantación de un conjunto adecuado de controles, ya sean políticas, prácticas, procedimientos, o estructuras organizativas, que aseguren que los sistemas de información no incurrir en riesgos asociados a la pérdida de confidencialidad, integridad o disponibilidad.

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, los riesgos a los que estén expuestos y las medidas de seguridad.

- La seguridad del sistema debe contemplar los aspectos de **prevención, detección y corrección**, para conseguir que las amenazas sobre el mismo no se materialicen, no afecten gravemente a la información que maneja, o los servicios que se prestan.

Las medidas de prevención deben eliminar o, al menos reducir, la posibilidad de que las amenazas lleguen a materializarse con perjuicio para el sistema. Estas medidas de prevención contemplarán, entre otras, la disuasión y la reducción de la exposición.

Las medidas de detección estarán acompañadas de medidas de reacción, de forma que los incidentes de seguridad se atajen a tiempo.

Las medidas de recuperación permitirán la restauración de la información y los servicios, de forma que se pueda hacer frente a las situaciones en las que un incidente de seguridad inhabilite los medios habituales.

Sin merma de los demás principios básicos y requisitos mínimos establecidos, el sistema garantizará la conservación de los datos e informaciones en soporte electrónico.

De igual modo, el sistema mantendrá disponibles los servicios durante todo el ciclo vital de la información digital, a través de una concepción y procedimientos que sean la base para la preservación del patrimonio digital.

- Los servicios deben estructurarse con diferentes **líneas de defensa**, constituidas por medidas de naturaleza organizativa, física y lógica, de modo que una amenaza que se materialice no pueda desarrollar todo su potencial y se mitigue, rápidamente, el daño producido.
- Las medidas de seguridad se **reevaluarán y actualizarán periódicamente**, para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección, llegando incluso a un replanteamiento de la seguridad, si fuese necesario.
- **Segregación de roles** para asegurar la calidad y evitar posibles conflictos de intereses, **asegurando la consistencia** de la seguridad, mediante actuaciones coordinadas entre todos los actores implicados.

Centro de Proceso de Datos
Av. Complutense. s/n. 28040 Madrid.

Código Seguro De Verificación	6339-5553-6D6BP3035-7477	Estado	Fecha y hora
Firmado Por	Jorge Jesus Gomez Sanz - Vicerrector de Tecnología y Sostenibilidad de la Universidad Complutense de Madrid Vice-Rector Of Technology And Sustainability Of The Universidad Complutense de Madrid	Firmado	06/04/2022 11:20:22
Observaciones		Página	8/18
Uri De Verificación	https://sede.ucm.es/verificacion?csv=6339-5553-6D6BP3035-7477		
Normativa	Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015).		





SE0001	Versión	Pág.
Política de Seguridad de la Información	2.0	9 de 18

- **No dejar lagunas de responsabilidades**, asegurando que el ciclo de vida de las medidas de seguridad esté cubierto: definición, implantación/operación, revisión y mejora.
- **Permitir la toma de decisiones** para hacer frente a los retos, problemas e incidencias relacionados con la seguridad de la información.

Centro de Proceso de Datos
Av. Complutense. s/n. 28040 Madrid.

Código Seguro De Verificación	6339-5553-6D6BP3035-7477	Estado	Fecha y hora	
Firmado Por	Jorge Jesus Gomez Sanz - Vicerrector de Tecnología y Sostenibilidad de la Universidad Complutense de Madrid Vice-Rector Of Technology And Sustainability Of The Universidad Complutense de Madrid	Firmado	06/04/2022 11:20:22	
Observaciones		Página	9/18	
Uri De Verificación	https://sede.ucm.es/verificacion?csv=6339-5553-6D6BP3035-7477			
Normativa	Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015).			



SE0001	Versión	Pág.
Política de Seguridad de la Información	2.0	10 de 18

7 OBJETIVOS EN SEGURIDAD

Para responder a la misión de protección de la información, se han establecido los siguientes objetivos:

1. GARANTIZAR UN NIVEL DE SERVICIO ADECUADO en cuanto a la disponibilidad, integridad, confidencialidad, autenticidad, trazabilidad y protección de la información de la UCM.

2. ASEGURAR UN CUMPLIMIENTO EFICIENTE DEL ESQUEMA NACIONAL DE SEGURIDAD, así como las restantes **OBLIGACIONES LEGALES Y LAS DIRECTRICES ADMINISTRATIVAS** en materia de seguridad que resulten aplicables a la UCM.

3. INCORPORAR LAS MEJORES PRÁCTICAS Y LA CALIDAD en las actuaciones y gestión de la seguridad para cumplir de forma sistemática, continua, eficaz y eficiente, **los objetivos de seguridad anteriores** frente a los cambios internos y externos.

Centro de Proceso de Datos
Av. Complutense. s/n. 28040 Madrid.

Código Seguro De Verificación	6339-5553-6D6BP3035-7477	Estado	Fecha y hora
Firmado Por	Jorge Jesus Gomez Sanz - Vicerrector de Tecnología y Sostenibilidad de la Universidad Complutense de Madrid Vice-Rector Of Technology And Sustainability Of The Universidad Complutense de Madrid	Firmado	06/04/2022 11:20:22
Observaciones		Página	10/18
Uri De Verificación	https://sede.ucm.es/verificacion?csv=6339-5553-6D6BP3035-7477		
Normativa	Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015).		





SE0001	Versión	Pág.
Política de Seguridad de la Información	2.0	11 de 18

8 ORGANIZACIÓN

Para poder alcanzar con éxito los objetivos referidos en el punto anterior, la UCM ha establecido una estructura de gestión **para coordinar y controlar de forma consistente y responsable** la implantación y la operativa de las medidas de seguridad de la información en la UCM:

- **Comité de Seguridad de la Información** para la toma de decisiones en relación a la seguridad de la información de la UCM.
- **Comités Técnicos de seguridad de la información** para la coordinación de las operaciones de la seguridad de los sistemas de información afectados por el ENS en la UCM.
- **Responsable de Seguridad:** será la persona encargada de la seguridad de la información manejada y de los servicios prestados por los sistemas de información, de acuerdo a lo establecido en la Política de Seguridad de la UCM. Recae sobre **el Vicerrectorado con competencias en Tecnologías de la Información**, quien designará un **Administrador de Protección de la Información** entre el personal de los Servicios Informáticos con funciones en el área de seguridad, con objeto de realizar y mantener la gestión de riesgos en el ámbito del ENS.
- **Responsable del Sistema:** será el encargado de desarrollar, operar y mantener los sistemas de información afectados por el ENS durante todo su ciclo de vida, para que tengan un correcto funcionamiento y asegurar que las medidas de seguridad de los sistemas se integran dentro del marco general de la Política de Seguridad. **Será la Dirección de los Servicios Informáticos, pudiendo delegar en los responsables de cada uno de los sistemas afectados.** Designará un **Administrador de Seguridad de Sistemas** entre el personal de los Servicios Informáticos con funciones en el área de seguridad, con objeto de ejecutar, gestionar y mantener las medidas de seguridad aplicables a los sistemas de información.
- **Responsable de la Información:** será la persona u órgano encargado de la protección de la información y que determinará los niveles de seguridad de la información de los activos incluidos en el ámbito del ENS en la UCM, conforme a la normativa vigente, previo informe del Responsable de Seguridad y del Responsable del Sistema. **Dicha responsabilidad recae sobre el Comité de Seguridad de la Información** quien designará los **Comités Técnicos** necesarios para asegurar la correcta implantación de las medidas de seguridad definidas.
- **Responsables de los Servicios:** serán los encargados de establecer los niveles de seguridad de los servicios incluidos en el ámbito del ENS en la UCM, previo informe del Responsable de Seguridad y del Responsable del Sistema. **Se corresponde con el Vicerrector, Gerente, Vicegerente o Director con competencias en el área.**
- **Responsable del Tratamiento:** La Universidad Complutense de Madrid, será la responsable final del tratamiento, y, quien determine, los fines y medios del tratamiento de los datos de carácter personal.
- **Delegada de Protección de Datos:** A fin de dar cumplimiento a lo requerido en el artículo 37 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, la Universidad Complutense de Madrid cuenta con una Delegada de Protección de Datos nombrada por el Rector, a quien le corresponden las funciones esenciales de asesoramiento y supervisión en materia de protección de datos junto con las demás establecidas en el artículo 39 del citado Reglamento, y las derivadas de la normativa española de protección de datos, así como de los documentos de buenas prácticas que se emitan por parte de la Agencia Española de Protección de Datos y del Comité Europeo de Protección de Datos.

Los conflictos entre las diferentes personas, unidades u órganos responsables que componen la estructura organizativa de la política de seguridad de la información serán resueltos por el superior jerárquico común,

Código Seguro De Verificación	6339-5553-6D6BP3035-7477	Estado	Fecha y hora
Firmado Por	Jorge Jesus Gomez Sanz - Vicerrector de Tecnología y Sostenibilidad de la Universidad Complutense de Madrid Vice-Rector Of Technology And Sustainability Of The Universidad Complutense de Madrid	Firmado	06/04/2022 11:20:22
Observaciones		Página	11/18
Url De Verificación	https://sede.ucm.es/verificacion?csv=6339-5553-6D6BP3035-7477		
Normativa	Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015).		





SE0001	Versión	Pág.
Política de Seguridad de la Información	2.0	12 de 18

que podrá elevar consulta previa al Comité de Seguridad de la Información. En caso de conflicto prevalecerán las decisiones del Comité de Seguridad de la Información.

En los conflictos entre las personas responsables que componen la estructura organizativa de la política de seguridad de la información y las personas responsables definidas en la normativa de protección de datos de carácter personal prevalecerá la decisión que presente un mayor nivel de exigencia respecto a la protección de los datos de carácter personal.

El detalle de la organización y de las responsabilidades se encuentra en el documento SE0002 Organización de la Seguridad de la Información.

9 ESTRUCTURACIÓN DE LA DOCUMENTACIÓN DE SEGURIDAD

La Política de Seguridad de la Información es de obligado cumplimiento y se estructura en los siguientes niveles relacionados jerárquicamente:

- 1) **Primer nivel:** Política de Seguridad de la Información.
- 2) **Segundo nivel:** Políticas de Seguridad de la Información.
- 3) **Tercer nivel:** Procedimientos e Instrucciones Técnicas de Seguridad de la Información.
- 4) **Cuarto nivel:** Informes, registros y evidencias electrónicas.

La estructura jerárquica permite adaptar con eficiencia los niveles inferiores a los cambios en los entornos operativos de UCM, sin necesidad de revisar su estrategia de seguridad.

El personal de UCM tendrá la obligación de conocer y cumplir, además de la Política de Seguridad de la Información, todas las Políticas, los Procedimientos e Instrucciones Técnicas de Seguridad de la Información que puedan afectar a sus funciones.

La Política de Seguridad de la Información, las Políticas de Seguridad, los Procedimientos e Instrucciones Técnicas de Seguridad de la Información estarán disponibles, siempre que se considere que su difusión es necesaria, para todos los empleados en la Intranet de UCM según vayan siendo aprobadas.

1) Primer nivel: Política de Seguridad de la Información

Este documento es de obligado cumplimiento por todo el personal, interno y externo, de UCM, recogido en el presente documento, revisado por el Comité de Seguridad de la Información de la UCM y aprobado por el Rector.

2) Segundo nivel: Políticas de Seguridad de la Información

De obligado cumplimiento de acuerdo con el ámbito organizativo, técnico o legal correspondiente.

La responsabilidad de aprobación de los documentos redactados en este nivel será competencia del Comité de Seguridad de la Información a propuesta del Responsable de Seguridad.

Código Seguro De Verificación	6339-5553-6D6BP3035-7477	Estado	Fecha y hora
Firmado Por	Jorge Jesus Gomez Sanz - Vicerrector de Tecnología y Sostenibilidad de la Universidad Complutense de Madrid Vice-Rector Of Technology And Sustainability Of The Universidad Complutense de Madrid	Firmado	06/04/2022 11:20:22
Observaciones		Página	12/18
Uri De Verificación	https://sede.ucm.es/verificacion?csv=6339-5553-6D6BP3035-7477		
Normativa	Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015).		





SE0001	Versión	Pág.
Política de Seguridad de la Información	2.0	13 de 18

3) Tercer nivel: Procedimientos e Instrucciones Técnicas de Seguridad de la Información

Documentos técnicos orientados a resolver las tareas, consideradas críticas por el perjuicio que causaría una actuación inadecuada, de seguridad, desarrollo, mantenimiento y explotación de los sistemas de información.

La responsabilidad de aprobación de los procedimientos e instrucciones técnicas es del Responsable de Seguridad bajo la supervisión y asesoramiento del Comité técnico.

4) Cuarto Nivel: Informes, registros y evidencias electrónicas

El cuarto nivel está constituido por documentos de carácter técnico que recogen el resultado y las conclusiones de un estudio o una valoración; documentos de carácter técnico que recogen amenazas y vulnerabilidades de los sistemas de información, así como también evidencias electrónicas generadas durante todas las fases del ciclo de vida del sistema de información.

La responsabilidad de que existan este tipo de documentos es del Responsable del Sistema.

5) Otra documentación

Se podrá seguir en todo momento los procedimientos, normas e instrucciones técnicas STIC, las guías CCN-STIC de las series 400, 500, 600 y 800, así como las guías, informes jurídicos y recomendaciones de la Agencia Española de Protección de Datos (AEPD).

Se aplicará en todo momento el bloque normativo vigente relativo a la seguridad y a la protección de datos personales, tanto procedente de la Unión Europea como del Estado Español.

Centro de Proceso de Datos
Av. Complutense. s/n. 28040 Madrid.

Código Seguro De Verificación	6339-5553-6D6BP3035-7477	Estado	Fecha y hora
Firmado Por	Jorge Jesus Gomez Sanz - Vicerrector de Tecnología y Sostenibilidad de la Universidad Complutense de Madrid Vice-Rector Of Technology And Sustainability Of The Universidad Complutense de Madrid	Firmado	06/04/2022 11:20:22
Observaciones		Página	13/18
Uri De Verificación	https://sede.ucm.es/verificacion?csv=6339-5553-6D6BP3035-7477		
Normativa	Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015).		





SE0001	Versión	Pág.
Política de Seguridad de la Información	2.0	14 de 18

10 REVISIÓN Y APROBACIÓN

La Política de Seguridad de la Información será revisada, al menos, cada dos años.

La presente Política de Seguridad de la Información fue aprobada por el Rector el día ___ de _____ de 2022.

Fdo.:

Cargo:

Centro de Proceso de Datos
Av. Complutense. s/n. 28040 Madrid.


Código Seguro De Verificación	6339-5553-6D6BP3035-7477	Estado	Fecha y hora
Firmado Por	Jorge Jesus Gomez Sanz - Vicerrector de Tecnología y Sostenibilidad de la Universidad Complutense de Madrid Vice-Rector Of Technology And Sustainability Of The Universidad Complutense de Madrid	Firmado	06/04/2022 11:20:22
Observaciones		Página	14/18
Uri De Verificación	https://sede.ucm.es/verificacion?csv=6339-5553-6D6BP3035-7477		
Normativa	Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015).		





SE0001	Versión	Pág.
Política de Seguridad de la Información	2.0	15 de 18

Centro de Proceso de Datos
Av. Complutense. s/n. 28040 Madrid.

Código Seguro De Verificación	6339-5553-6D6BP3035-7477	Estado	Fecha y hora	
Firmado Por	Jorge Jesus Gomez Sanz - Vicerrector de Tecnología y Sostenibilidad de la Universidad Complutense de Madrid Vice-Rector Of Technology And Sustainability Of The Universidad Complutense de Madrid	Firmado	06/04/2022 11:20:22	
Observaciones		Página	15/18	
Uri De Verificación	https://sede.ucm.es/verificacion?csv=6339-5553-6D6BP3035-7477			
Normativa	Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015).			



SE0001	Versión	Pág.
Política de Seguridad de la Información	2.0	16 de 18

11 ANEXO I. REQUISITOS DE SEGURIDAD DE OBLIGADO CUMPLIMIENTO

Para la correcta implementación y cumplimiento de la presente Política de Seguridad de la Información es necesario aplicar una serie de requisitos de obligado cumplimiento:

1.1 La seguridad en la Organización

La seguridad comprometerá a todos los miembros de UCM, sin excepción.

En el apartado 8 (Organización) del presente documento, se especifica la Organización de la seguridad con la definición de la estructura organizativa.

Asimismo, la implementación de dicha organización está en el marco normativo cubierto por el establecimiento de un sistema de Gestión de la Seguridad, basado en el ENS.

1.2 Análisis y Gestión de riesgos

Los servicios e infraestructuras bajo el alcance de la presente Política estarán sometidos a un análisis de riesgos para orientar las medidas de protección a minimizar los mismos.

La descripción de la metodología y evaluación del riesgo están desarrollados en “Metodología de análisis y gestión de riesgos”.

El análisis de riesgos se realizará igualmente cuando se vaya a iniciar o a modificar un tratamiento de datos de carácter personal, en línea a lo establecido en el Reglamento General de Protección de Datos. En estos casos se contemplarán en el alcance del análisis todos aquellos activos que intervengan en el tratamiento, considerando tanto activos relacionados con los sistemas de información, como humanos, locales o terceros.

A raíz de los resultados obtenidos en los mencionados análisis de riesgos de los servicios y de los tratamientos de datos personales, se determinarán las medidas necesarias para proteger dichos datos.

1.3 Gestión de personal

En las políticas de uso interno, se detallarán la obligatoriedad de conocimiento y concienciación en materia de seguridad según sus responsabilidades. Los recursos necesarios para la implementación del sistema de seguridad, así como aquellos que lleven a cabo su operación, mantenimiento, supervisión, o tenga relación con el sistema se establece anualmente en los planes estratégicos de la UCM.

El Responsable de Recursos Humanos incluirá las funciones relativas a la seguridad de la información en las descripciones de puestos de trabajo, informará a todo el personal nuevo que ingrese en la UCM o cambie de ubicación de sus obligaciones con respecto del cumplimiento de la Política de Seguridad de la Información, gestionará las cláusulas de confidencialidad. La Unidad de Seguridad y Protección de la Información, la Oficina de Protección de datos y la Unidad de formación coordinarán las tareas de concienciación y formación respecto de la presente Política.

Periódicamente se realizarán evaluaciones de desempeño y seguimiento del personal.

1.4 Profesionalidad

En las políticas internas se detallarán las funciones, las responsabilidades del personal, así como los objetivos de las acciones de formación y concienciación.

Periódicamente se diseñará un plan de formación específico en el que se tiene en cuenta las necesidades de profesionalización del sistema de seguridad.

Centro de Proceso de Datos
Av. Complutense. s/n. 28040 Madrid.

Código Seguro De Verificación	6339-5553-6D6BP3035-7477	Estado	Fecha y hora
Firmado Por	Jorge Jesus Gomez Sanz - Vicerrector de Tecnología y Sostenibilidad de la Universidad Complutense de Madrid Vice-Rector Of Technology And Sustainability Of The Universidad Complutense de Madrid	Firmado	06/04/2022 11:20:22
Observaciones		Página	16/18
Url De Verificación	https://sede.ucm.es/verificacion?csv=6339-5553-6D6BP3035-7477		
Normativa	Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015).		





SE0001	Versión	Pág.
Política de Seguridad de la Información	2.0	17 de 18

1.5 Autorización y control de Acceso

El acceso a los sistemas de información estará restringido y limitado a aquellos usuarios o procesos que lo necesiten para el desarrollo de su actividad y estén previamente autorizados.

El acceso a la información seguirá el principio de “necesidad de conocer”, de forma que los privilegios otorgados a cada identidad sean los mínimos imprescindibles para el desarrollo de su actividad.

La identificación de los usuarios será tal que se pueda conocer en todo momento quién recibe derechos de accesos y quién ha realizado alguna actividad, por lo que los identificadores deberán ser personales, no compartidos, e intransferibles.

Los lugares con acceso restringido igualmente deberán estar controlados y previamente autorizados por los responsables asignados.

1.6 Protección de las instalaciones

Los sistemas de información se ubicarán en zonas protegidas, con acceso restringido, habilitado únicamente al personal autorizado.

1.7 Adquisición de productos

Para el proceso de adquisición de nuevos productos, sistemas o servicios se establecerán protocolos de análisis de riesgos con proveedores y se mantendrán actualizados los listados de proveedores habituales. Las adquisiciones deben ser autorizadas por los responsables del área implicada y el Servicio de Contratación cumpliendo la normativa vigente de contratación para la UCM, y a través de informes favorables del proveedor, en caso de requerirse. Cuando proceda, se suscribirán los correspondientes contratos con los encargados de tratamiento, conforme a lo dispuesto en el art. 28 del RGPD.

1.8 Seguridad por Defecto

Los sistemas y aplicaciones se diseñarán y construirán bajo el principio de seguridad por defecto, de tal forma que:

- El sistema ofrecerá la funcionalidad mínima necesaria, y ninguna adicional. Cualquier función que no sea de interés o innecesaria será deshabilitada o no implementada.
- La operación y explotación de los sistemas estará limitada a aquellas personas o ubicaciones que se autoricen, quedando prohibidas para el resto.
- El uso del sistema ha de ser seguro, de tal forma que el uso inseguro requiera intención por parte del usuario.

La seguridad estará presente desde la concepción de un sistema o aplicación y permanecerá presente durante todo su ciclo de vida.

En la concepción de un nuevo sistema o aplicación, o modificación sustancial de un sistema o aplicación existente, se contará siempre, y desde el inicio, con la participación del Responsable de la Información y del Servicio, del Responsable de Seguridad de la Información y del Delegado de Protección de Datos.

1.9 Integridad y actualización del sistema

Se seguirán en todo momento las informaciones acerca de las vulnerabilidades que afectan a los sistemas de información.

Se seguirán las recomendaciones de los fabricantes de equipos y software en cuanto a actualizaciones de seguridad, que deberán ser analizadas en cuanto a su idoneidad y conveniencia, y aplicadas en caso positivo con la menor dilación.

Código Seguro De Verificación	6339-5553-6D6BP3035-7477	Estado	Fecha y hora
Firmado Por	Jorge Jesus Gomez Sanz - Vicerrector de Tecnología y Sostenibilidad de la Universidad Complutense de Madrid Vice-Rector Of Technology And Sustainability Of The Universidad Complutense de Madrid	Firmado	06/04/2022 11:20:22
Observaciones		Página	17/18
Uri De Verificación	https://sede.ucm.es/verificacion?csv=6339-5553-6D6BP3035-7477		
Normativa	Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015).		





SE0001	Versión	Pág.
Política de Seguridad de la Información	2.0	18 de 18

1.10 Protección de la Información Almacenada y en Tránsito

Se protegerán los entornos que contienen información almacenada y en tránsito entre entornos inseguros. En este sentido se protegerán convenientemente los equipos portátiles que puedan contener información, así como los soportes extraíbles (pendrives, discos duros extraíbles, etc.).

En el caso de la existencia de una normativa de protección de la información, más restrictiva, se dará cumplimiento a la misma. Esta normativa puede ser interna o externa a la UCM.

1.11 Prevención ante otros sistemas de información interconectados

Se desplegarán las protecciones necesarias para proteger el perímetro de la red corporativa de la UCM, de forma que se neutralicen las posibles intrusiones procedentes del exterior, ya sea iniciadas malintencionadamente por terceros o como consecuencia de la interconexión con sistemas de terceros.

1.12 Registro de Actividad

Los sistemas y aplicaciones generarán los registros de actividad necesarios para conocer la actividad en los sistemas, de forma que se pueda determinar en todo momento qué persona actúa, sobre qué datos, con qué operaciones y sus privilegios de acceso.

1.13 Gestión de Incidentes de Seguridad

La UCM definirá e implantará procedimientos de gestión de incidentes de seguridad que aseguren la correcta gestión y respuesta efectiva que permita anular o minimizar el impacto del incidente en la información, los servicios, los empleados, los usuarios y, en general, en la actividad de la UCM.

El procedimiento de comunicación, gestión y respuesta a incidentes de seguridad contemplará la comunicación y notificación de los incidentes a los organismos receptores de dicha información, de acuerdo con la legalidad vigente.

En caso de violación de la seguridad de los datos personales, el responsable del tratamiento la notificará a la autoridad de control (Agencia Española de Protección de Datos) sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, en los términos establecidos en el artículo 33 del RGPD.

Así mismo y cuando sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento la comunicará al interesado sin dilación indebida de conformidad con lo previsto en el artículo 34 del RGPD.

1.14 Continuidad de la Actividad

Para asegurar la disponibilidad de los servicios y sistemas de información, la UCM diseñará e implantará Planes de Continuidad de Servicio que eviten las interrupciones de las actividades de la UCM y garanticen, ante una contingencia, la reanudación de los servicios y sistemas de información a los niveles adecuados de operatividad.

1.15 Gestión de la Seguridad y Mejora Continua

Se deberá establecer un Sistema de Gestión de la Seguridad que permita conocer en cada momento el estado de la seguridad, mediante la definición y medida de indicadores, y permita tomar las decisiones informadas pertinentes para cumplir los requisitos de seguridad establecidos.

Se establecerá un proceso de mejora continua mediante el análisis de la situación, la implantación de nuevas medidas de seguridad, la mejora de las existentes y la aportación de mejoras sugeridas por el Comité de Seguridad de la Información y por toda la UCM en su conjunto.

Código Seguro De Verificación	6339-5553-6D6BP3035-7477	Estado	Fecha y hora
Firmado Por	Jorge Jesus Gomez Sanz - Vicerrector de Tecnología y Sostenibilidad de la Universidad Complutense de Madrid Vice-Rector Of Technology And Sustainability Of The Universidad Complutense de Madrid	Firmado	06/04/2022 11:20:22
Observaciones		Página	18/18
Uri De Verificación	https://sede.ucm.es/verificacion?csv=6339-5553-6D6BP3035-7477		
Normativa	Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015).		

