Universidad Complutense de Madrid
Servicios Informáticos
Unidad de Seguridad y Protección de la Información

Documentos

UCM Serie:

Seguridad

# SE0001 Política de Seguridad de la Información

Versión del Documento 3.1

24-06-2024

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. 2



| Código Seguro De Verificación | 654F-3765-4733P3046-5832 | 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 Sustainablity Of The Universidad Complutense de Madrid | Firmado | 01/07/2024 13:07:04 |
| Observaciones | | Página | 1/21 |
| Url De Verificación | https://sede.ucm.es/verificacion?csv=654F-3765-4733P3046-5832 | | |
| Normativa | Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015). | | |

***HOJA DE CONTROL***

| Elaborado por | Revisado por | Aprobado por |
|---|---|---|
| USPI | CSI | CSI |

***HISTORIAL DE CAMBIOS***

| Versión | Fecha | Autor | Descripción |
|---|---|---|---|
| 1.0 | 01/04/2014 | USPI | Documento inicial |
| 2.0 | 14.02.2022 | USPI | Actualización de referencias normativas |
| 3.0 | 08/03/2024 | USPI | Actualización de directrices de seguridad |
| 3.1 | 24/06/2024 | USPI | Gestión de cambios aplicado |





| Código Seguro De Verificación | 654F-3765-4733P3046-5832 | 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 Sustainablity Of The Universidad Complutense de Madrid | Firmado | 01/07/2024 13:07:04 |
| Observaciones | | Página | 2/21 |
| Url De Verificación | https://sede.ucm.es/verificacion?csv=654F-3765-4733P3046-5832 | | |
| Normativa | Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015). | | |

# INDICE







| Código Seguro De Verificación | 654F-3765-4733P3046-5832 | 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 Sustainablity Of The Universidad Complutense de Madrid | Firmado | 01/07/2024 13:07:04 |
| Observaciones | | Página | 3/21 |
| Url De Verificación | https://sede.ucm.es/verificacion?csv=654F-3765-4733P3046-5832 | | |
| Normativa | Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015). | | |

# 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 12 del Real Decreto 311/2022 de 3 de mayo, 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.

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.




| Código Seguro De Verificación | 654F-3765-4733P3046-5832 | 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 Sustainablity Of The Universidad Complutense de Madrid | Firmado | 01/07/2024 13:07:04 |
| Observaciones | | Página | 4/21 |
| Url De Verificación | https://sede.ucm.es/verificacion?csv=654F-3765-4733P3046-5832 | | |
| Normativa | Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015). | | |

## 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 es aplicable con carácter obligatorio a toda la organización, así como aquellas empresas que colaboren con la Universidad y hagan uso de la información y de los sistemas de información que sean propiedad de la UCM para el desarrollo de sus funciones en cualquier momento del ciclo de vida de la información.

## 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 |
| ASS | Administrador de la Seguridad del Sistema |
| API | Administrador de Protección de la Información |
| USPI | Unidad de Seguridad y Protección de la Información |




| Código Seguro De Verificación | 654F-3765-4733P3046-5832 | 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 Sustainablity Of The Universidad Complutense de Madrid | Firmado | 01/07/2024 13:07:04 |
| Observaciones | | Página | 5/21 |
| Url De Verificación | https://sede.ucm.es/verificacion?csv=654F-3765-4733P3046-5832 | | |
| Normativa | Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015). | | |

## 4. LEGISLACIÓN APLICABLE

El marco normativo de seguridad que afecta al desarrollo de las actividades y competencias de la UCM está constituido por normas jurídicas de ámbito europeo, estatal, autonómico y universitario enfocadas a la administración electrónica, seguridad de la información, ciberseguridad y los servicios que la gestionan, así como a la protección de datos personales.

Las normas jurídicas que se encuentran recogidas en el presente apartado forman parte del marco legal y regulatorio aplicable a la UCM:

- 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.
- Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.
- 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 56/2007 de Medidas de Impulso de la Sociedad de la Información.
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad 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-ISO 10013:2021 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).
- DTI-USPI-doc-Metodología de Análisis y Gestión de Riesgos.
- 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 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 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.




| Código Seguro De Verificación | 654F-3765-4733P3046-5832 | 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 Sustainablity Of The Universidad Complutense de Madrid | Firmado | 01/07/2024 13:07:04 |
| Observaciones | | Página | 6/21 |
| Url De Verificación | https://sede.ucm.es/verificacion?csv=654F-3765-4733P3046-5832 | | |
| Normativa | Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015). | | |

GUIAS DE REFENCIAS

- CCN-STIC-801: ENS - Responsabilidades y funciones en el ENS.
- CCN-STIC-805: ENS - Política de Seguridad de la Información.
- CCN-STIC 881: ENS – Perfil de Cumplimiento Específico Universidades
- CCN-STIC-201: Organización y gestión para la seguridad de las TIC.
- Guía CCN-STIC-401: Glosario de términos.

## 5. 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 entiende como un **proceso integral** constituido por todos los elementos técnicos, humanos, materiales, jurídicos 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 la de los responsables jerárquicos, para evitar que, la ignorancia, la falta de organización y de coordinación o de instrucciones adecuadas, constituyan 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 incurren 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 una apropiada aplicación de medidas de seguridad, de manera equilibrada y proporcionada a la naturaleza de la información tratada, de los servicios a prestar y de los riesgos a los que estén expuestos.
- La seguridad del sistema debe contemplar las acciones relativas a los aspectos de **prevención, detección y respuesta**, al objeto de minimizar sus vulnerabilidades y lograr que las amenazas sobre el mismo no se materialicen o que, en el caso de hacerlo, no afecten gravemente a la información que maneja o a los servicios que presta.
  - Las **medidas de prevención**, que podrán incorporar componentes orientados a la disuasión o a la reducción de la superficie de exposición, deben eliminar o reducir la posibilidad de que las amenazas lleguen a materializarse.
  - Las **medidas de detección** irán dirigidas a descubrir la presencia de un ciber incidente.
  - Las **medidas de respuesta**, que se gestionarán en tiempo oportuno, estarán orientadas a la restauración de la información y los servicios que pudieran haberse visto afectados por un incidente de seguridad.

  Además de los principios básicos y requisitos mínimos establecidos, el sistema de información garantizará la conservación de los datos e información en soporte electrónico.
  De igual modo, la Dirección de la UCM velará por mantener 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.




| Código Seguro De Verificación | 654F-3765-4733P3046-5832 | 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 Sustainablity Of The Universidad Complutense de Madrid | Firmado | 01/07/2024 13:07:04 |
| Observaciones | | Página | 7/21 |
| Url De Verificación | https://sede.ucm.es/verificacion?csv=654F-3765-4733P3046-5832 | | |
| Normativa | Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015). | | |

- 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.
- La seguridad del sistema debe contar con **vigilancia continua y reevaluación periódica** de forma que:
    - La **vigilancia continua** permitirá la detección de actividades o comportamientos anómalos y su oportuna respuesta.
    - La **evaluación permanente** del estado de la seguridad de los activos permitirá medir su evolución, detectando vulnerabilidades e identificando deficiencias de configuración.
    - Las medidas de seguridad se **reevaluarán y actualizarán periódicamente**, adecuando su eficacia a la evolución de los riesgos y los sistemas de protección, pudiendo llegar a un replanteamiento de la seguridad, si fuese necesario.
- La **diferenciación de responsabilidades** garantiza la segregación de roles para asegurar la calidad y evitar posibles conflictos de intereses, fortaleciendo la consistencia de la seguridad, mediante actuaciones coordinadas entre todos los actores implicados.
- **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.




| Código Seguro De Verificación | 654F-3765-4733P3046-5832 | 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 Sustainablity Of The Universidad Complutense de Madrid | Firmado | 01/07/2024 13:07:04 |
| Observaciones | | Página | 8/21 |
| Url De Verificación | https://sede.ucm.es/verificacion?csv=654F-3765-4733P3046-5832 | | |
| Normativa | Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015). | | |

## 6. COMPROMISO DE LA DIRECCIÓN

La Dirección de la UCM reconoce que la información es un activo fundamental de la organización y establece que su protección es un objetivo prioritario para el adecuado cumplimiento de los servicios que presta.

La Política de Seguridad de la Información de la UCM define la intención y el compromiso expreso de la Dirección para establecer las directrices y proveer de los medios necesarios para gestionar la seguridad de manera eficiente y dar cumplimiento a la legislación aplicable en materia de seguridad de la información.

## 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.




| Código Seguro De Verificación | 654F-3765-4733P3046-5832 | 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 Sustainablity Of The Universidad Complutense de Madrid | Firmado | 01/07/2024 13:07:04 |
| Observaciones | | Página | 9/21 |
| Url De Verificación | https://sede.ucm.es/verificacion?csv=654F-3765-4733P3046-5832 | | |
| Normativa | Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015). | | |

# 8. ORGANIZACIÓN DE LA SEGURIDAD

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.

La estructura organizativa de seguridad de la información de la UCM está compuesta por las siguientes figuras:

- **COMITÉ DE SEGURIDAD DE LA INFORMACIÓN:** Encargado de la toma de decisiones en relación con la seguridad de la información de la UCM. Su objetivo es gestionar y mejorar progresivamente la seguridad, entregando respuesta a los distintos riesgos. Este comité está constituido por representantes de distintas áreas de gobierno de la UCM y se reunirá periódicamente al menos semestralmente, o cuando existan propuestas o eventos que lo justifiquen, y podrá invitar a personas de otras áreas de la UCM, o a especialistas externos cuando lo estime oportuno.

  El Comité de Seguridad de la Información estará presidido por el Vicerrectorado con competencias en Tecnologías de la Información y por los siguientes vocales:

  - El Secretario General o persona en quien delegue.
  - El Gerente o persona en quien delegue.
  - El titular del órgano con competencias en seguridad física o persona en quien delegue.
  - El Delegado de Protección de Datos o persona en quien delegue.
  - El Director de los Servicios Informáticos o persona en quien delegue, que actuará como Secretario.
  - El Director de Administración Electrónica o persona en quien delegue.
  - El Decano de la Facultad de Informática o persona en quien delegue.

  **FUNCIONES:**

  Corresponde al Comité de Seguridad de la Información:

  - Elaborar y revisar regularmente la Política de Seguridad de la Información para su aprobación por el Rector, en los términos establecidos en el artículo 12 del RD 311/2022 de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
  - Aprobar la normativa interna en el ámbito de la seguridad de la información que sea necesaria.
  - Aprobar el Plan de Adecuación al Esquema Nacional de Seguridad y las medidas necesarias para su implantación.
  - Velar porque la seguridad de la información se tenga en cuenta en todos los proyectos de Tecnología de la Información (TI), desde su especificación inicial hasta su puesta en operación. En particular deberá velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas TI.
  - Promover la realización de las auditorías periódicas, que permitan verificar el cumplimiento de las obligaciones en materia de seguridad que establezca la Política de Seguridad y la normativa vigente.
  - Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables o entre diferentes áreas de la UCM.




| Código Seguro De Verificación | 654F-3765-4733P3046-5832 | 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 Sustainablity Of The Universidad Complutense de Madrid | Firmado | 01/07/2024 13:07:04 |
| Observaciones | | Página | 10/21 |
| Url De Verificación | https://sede.ucm.es/verificacion?csv=654F-3765-4733P3046-5832 | | |
| Normativa | Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015). | | |

- Recabar de los responsables de los distintos ámbitos de la seguridad informes regulares del estado de la seguridad de la Universidad y de las posibles incidencias que se produzcan.
- Este comité está constituido por representantes de distintas áreas de gobierno de la UCM y se reunirá periódicamente al menos trimestralmente, o cuando existan propuestas o eventos que lo justifiquen, y podrá invitar a personas de otras áreas de la UCM, o a especialistas externos cuando lo estime oportuno.

- **COMITÉS TECNICOS 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. El CSI creará cuantos Comités Técnicos de Seguridad de la Información estime necesarios para coordinar las operaciones de la seguridad de los sistemas de información afectados por el ENS en la UCM entre los diferentes departamentos técnicos responsables de su implantación y seguimiento, con las siguientes funciones:

  - Consensuar y acordar las funciones y tareas específicas de cada área.
  - Acordar métodos y procesos.
  - Implementar y respaldar las iniciativas aprobadas por el CSI.
  - Evaluar y reportar la conformidad con las directrices y los objetivos establecidos.
  - Revisar y reportar las incidencias de seguridad.
  - Revisar y evaluar la documentación.

  Estos comités, constituidos por representantes de distintas áreas técnicas de la UCM, se reunirán periódicamente, y siempre antes que el CSI, y podrán invitar a personas de otras áreas de la UCM, o a especialistas externos cuando lo estimen oportuno.

- **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 con 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.

  **FUNCIONES:**

  - Determinará la categoría del sistema, elaborará la declaración de aplicabilidad y decidirá sobre las medidas de seguridad adicionales.
  - Elaborará la configuración de seguridad que aplicará el ASS.
  - Recae bajo su responsabilidad aprobar los procedimientos operativos de seguridad elaborados por el Responsable del Sistema.
  - Tiene el deber de verificar el estado de la seguridad del sistema monitorizado por el ASS y el API.
  - Elaborará junto con el Responsable del Sistema los planes de mejora de la seguridad.
  - Es su deber promover la formación y concienciación, en materia de seguridad de la información, para la Comunidad Universitaria.
  - Es su responsabilidad la validación de los planes de continuidad elaborados por el Responsable del Sistema.
  - Recibe los informes sobre el grado de implantación y eficacia de las medidas de seguridad físicas e incidentes sobre las mismas del Responsable de la Seguridad Física.




| Código Seguro De Verificación | 654F-3765-4733P3046-5832 | 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 Sustainablity Of The Universidad Complutense de Madrid | Firmado | 01/07/2024 13:07:04 |
| Observaciones | | Página | 11/21 |
| Url De Verificación | https://sede.ucm.es/verificacion?csv=654F-3765-4733P3046-5832 | | |
| Normativa | Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015). | | |

- Debe verificar la seguridad en el ciclo de vida de los sistemas: especificación, arquitectura, desarrollo, operación y cambios, previo informe del Responsable del Sistema.

**DELEGACIÓN DE FUNCIONES:**

- Podrá designar cuantos Responsables de Seguridad delegados considere necesarios, aunque la responsabilidad final sigue recayendo sobre sí mismo.
- Los delegados se harán cargo, en su ámbito, de todas aquellas acciones que delegue el Responsable de la Seguridad.
- Cada delegado tendrá una dependencia funcional directa del Responsable de la Seguridad, que es a quien reporta.

- **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.

  **FUNCIONES:**

  - Desarrollar, operar y mantener los sistemas de información afectados por el ENS durante todo su ciclo de vida: especificaciones, instalación y verificación de su correcto funcionamiento.
  - Definir la topología y sistema de gestión de dichos sistemas de información estableciendo los criterios de uso y los servicios disponibles en los mismos.
  - Elaborar los procedimientos operativos de seguridad que deberán ser aprobados por el Responsable de Seguridad y aplicados por el API y el ASS.
  - Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.
  - Elaborar junto con el Responsable de Seguridad los planes de mejora de la seguridad.
  - Elaborar los planes de continuidad para los sistemas afectados (NIVEL ALTO) y realizar los simulacros correspondientes.
  - Puede decidir, de manera cautelar, 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. Comunicará dichas suspensiones temporales al Responsable de Seguridad y al Responsable del Servicio afectado.

  **DELEGACIÓN DE FUNCIONES:**

  - Podrá designar cuantos Responsables de Sistema delegados considere necesarios, aunque la responsabilidad final sigue recayendo sobre sí mismo.
  - Los delegados se harán cargo, en su ámbito, de todas aquellas acciones que delegue el Responsable del Sistema relacionadas con el desarrollo, la operación, mantenimiento, instalación y verificación del correcto funcionamiento del sistema de información. Se podrán encargar de subsistemas de información de cierta envergadura o de sistemas de información que presten servicios horizontales.




| Código Seguro De Verificación | 654F-3765-4733P3046-5832 | 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 Sustainablity Of The Universidad Complutense de Madrid | Firmado | 01/07/2024 13:07:04 |
| Observaciones | | Página | 12/21 |
| Url De Verificación | https://sede.ucm.es/verificacion?csv=654F-3765-4733P3046-5832 | | |
| Normativa | Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015). | | |

- Cada delegado tendrá una dependencia funcional directa del Responsable del Sistema, que es a quien reporta.

- **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.

  **FUNCIONES:**

  - Sobre ellos recae la responsabilidad última del uso que se haga de una cierta información y, por tanto, de su protección ante un incidente de seguridad.
  - Establece los requisitos de la información en materia de seguridad: determina los niveles de seguridad en cada dimensión de seguridad que se realizará dentro del marco establecido en el Anexo I del ENS.
  - Participa junto con los Responsables de los Servicios de la aceptación final del riesgo residual.
  - Los criterios de valoración estarán respaldados por la Política de Seguridad de la UCM en la medida en que sean sistemáticos, sin perjuicio de que puedan darse criterios particulares en casos singulares.

- **RESPONSABLE 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.**

  **FUNCIONES:**

  - Establecen los requisitos del servicio en materia de seguridad: determina los niveles de seguridad en cada dimensión de seguridad que debe realizarse dentro del marco establecido en el Anexo I del ENS.
  - Participan junto con los Responsables de la Información de la aceptación final del riesgo residual.
  - Los criterios de valoración estarán respaldados por la Política de Seguridad de la UCM en la medida en que sean sistemáticos, sin perjuicio de que puedan darse criterios particulares en casos singulares.
  - La prestación de un servicio siempre debe atender a las necesidades de seguridad de la información que maneja, es decir, hereda sus requisitos de seguridad y el responsable tiene la potestad de añadir otros relacionados con la disponibilidad, accesibilidad, interoperabilidad, etc.




| Código Seguro De Verificación | 654F-3765-4733P3046-5832 | 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 Sustainablity Of The Universidad Complutense de Madrid | Firmado | 01/07/2024 13:07:04 |
| Observaciones | | Página | 13/21 |
| Url De Verificación | https://sede.ucm.es/verificacion?csv=654F-3765-4733P3046-5832 | | |
| Normativa | Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015). | | |

- **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.

  **FUNCIONES:**

  - Garantizar la observancia de los principios relativos al tratamiento y aprobar la normativa concerniente a la protección de datos personales.
  - Designar al Delegado de Protección de Datos, cuando corresponda.
  - Adoptar las medidas técnicas y organizativas necesarias para garantizar la seguridad de los datos personales y evitar su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural. En particular, difundirá entre el personal las normas de seguridad que afecten al desarrollo de sus funciones, así como las consecuencias en que pudieran incurrir en caso de incumplimiento.
  - Garantizar el cumplimiento de las políticas y procedimientos aprobadas e implementadas en la UCM en materia de protección de datos.
  - Realizar evaluaciones del impacto en la protección de datos personales, cuando corresponda.
  - Asegurar que la realización de tratamientos por cuenta de terceras partes esté regulada en un contrato, que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que la persona encargada del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará (ni siquiera para su conservación) a otras personas.

- **DELEGADO 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 un Delegado de Protección de Datos nombrado 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.

  **FUNCIONES:**

  - Velar por que la UCM cumpla la normativa de protección de datos (RPGD) y respete los derechos de los ciudadanos.
  - Supervisar el cumplimiento de lo dispuesto en el RGPD, de otras disposiciones de protección de datos y de las políticas y procedimientos en materia de protección de datos personales adoptadas por la UCM, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes.
  - Informar y asesorar a la Dirección de la UCM y a los empleados de la UCM que se ocupen del tratamiento de las obligaciones que les incumben en virtud del RGPD y de otras disposiciones de protección de datos.
  - Asesorar acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación.




| Código Seguro De Verificación | 654F-3765-4733P3046-5832 | 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 Sustainablity Of The Universidad Complutense de Madrid | Firmado | 01/07/2024 13:07:04 |
| Observaciones | | Página | 14/21 |
| Url De Verificación | https://sede.ucm.es/verificacion?csv=654F-3765-4733P3046-5832 | | |
| Normativa | Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015). | | |

- Cooperar con la Autoridad de control, es decir, con la Agencia Española de Protección de Datos.
- Actuar como punto de contacto de la Autoridad de Control, es decir, con la Agencia Española de Protección de Datos.
- Además, asesorará y supervisión en las siguientes áreas:
  - Cumplimiento de principios relativos al tratamiento, como los de limitación en la finalidad, minimización o exactitud de los datos.
  - Identificación de las bases jurídicas de los tratamientos.
  - Valoración de la compatibilidad de finalidades distintas de las que originaron la recogida inicial de los datos.
  - Existencia de normativa sectorial que pueda determinar condiciones de tratamiento específicas, distintas de las establecidas por la normativa general de protección de datos.
  - Diseño e implantación de medidas de información a los afectados por los tratamientos de datos.
  - Establecimiento de mecanismos de recepción y gestión de solicitudes de ejercicio de
  - derechos por parte de los interesados.
  - Valoración de las solicitudes de ejercicio de derechos por parte de los interesados.
  - Contratación de encargados de tratamiento, incluido el contenido de los contratos o actos jurídicos que regulen la relación entre la UCM y los encargados del tratamiento.

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, 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.




| Código Seguro De Verificación | 654F-3765-4733P3046-5832 | 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 Sustainablity Of The Universidad Complutense de Madrid | Firmado | 01/07/2024 13:07:04 |
| Observaciones | | Página | 15/21 |
| Url De Verificación | https://sede.ucm.es/verificacion?csv=654F-3765-4733P3046-5832 | | |
| Normativa | Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015). | | |

# 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:** Normativas 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 Normativas, los Procedimientos e Instrucciones Técnicas de Seguridad de la Información que puedan afectar a sus funciones.

La Política de Seguridad de la Información, las Normativas 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. A continuación, se detallan los niveles definidos:

**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: Normativas 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.

**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.




| Código Seguro De Verificación | 654F-3765-4733P3046-5832 | 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 Sustainablity Of The Universidad Complutense de Madrid | Firmado | 01/07/2024 13:07:04 |
| Observaciones | | Página | 16/21 |
| Url De Verificación | https://sede.ucm.es/verificacion?csv=654F-3765-4733P3046-5832 | | |
| Normativa | Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015). | | |

## 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 entrará en Vigor desde la fecha de aprobación por el CSI.

Fdo.: Cargo:





| Código Seguro De Verificación | 654F-3765-4733P3046-5832 | 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 Sustainablity Of The Universidad Complutense de Madrid | Firmado | 01/07/2024 13:07:04 |
| Observaciones | | Página | 17/21 |
| Url De Verificación | https://sede.ucm.es/verificacion?csv=654F-3765-4733P3046-5832 | | |
| Normativa | Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015). | | |

# 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:

## 11.1. 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.

Cuando se deba externalizar un servicio, salvo por causa justificada y documentada, la organización prestataria de dicho servicio deberá designar Punto o Persona de Contacto para la seguridad de la información tratada y el servicio prestado, contando con el soporte y supervisión de los órganos de dirección, para cumplir con los requisitos de seguridad del servicio prestado, con las comunicaciones respecto a la seguridad de la información y la gestión de los incidentes que el servicio pueda tener.

## 11.2. 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.

## 11.3. 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




| Código Seguro De Verificación | 654F-3765-4733P3046-5832 | 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 Sustainablity Of The Universidad Complutense de Madrid | Firmado | 01/07/2024 13:07:04 |
| Observaciones | | Página | 18/21 |
| Url De Verificación | https://sede.ucm.es/verificacion?csv=654F-3765-4733P3046-5832 | | |
| Normativa | Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015). | | |

concienciación y formación respecto de la presente Política. Periódicamente se realizarán evaluaciones de desempeño y seguimiento del personal.

### 11.4. 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.

### 11.5. Autorización y control de los accesos

El acceso a los sistemas de información estará restringido y limitado a aquellos usuarios, procesos, dispositivos u otros sistemas de información 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.

### 11.6. Protección de las instalaciones

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

### 11.7. Adquisición de productos de seguridad y contratación de servicios de seguridad

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.

### 11.8. Mínimo privilegio

Los sistemas y aplicaciones se diseñarán y construirán otorgando los mínimos privilegios necesarios para su correcto desempeño, de tal forma que:

- El sistema ofrecerá la funcionalidad imprescindible para que la organización alcance sus objetivos competenciales o contractuales. 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 sencillo y seguro, de tal forma que el uso inseguro requiera intención por parte del usuario.




| Código Seguro De Verificación | 654F-3765-4733P3046-5832 | 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 Sustainablity Of The Universidad Complutense de Madrid | Firmado | 01/07/2024 13:07:04 |
| Observaciones | | Página | 19/21 |
| Url De Verificación | https://sede.ucm.es/verificacion?csv=654F-3765-4733P3046-5832 | | |
| Normativa | Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015). | | |

- Se aplicarán guías de configuración de seguridad para las diferentes tecnologías, adaptadas a la categorización del sistema, al efecto de eliminar o desactivar las funciones que sean innecesarias o inadecuadas.

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.

### 11.9. Integridad y actualización del sistema

La inclusión de cualquier elemento físico o lógico en el catálogo actualizado de activos del sistema, o su modificación, requerirá autorización formal previa.

Mediante evaluaciones y monitorización permanentes, se permitirá adecuar el estado de seguridad de los sistemas atendiendo a las deficiencias de configuración, las vulnerabilidades identificadas y las actualizaciones que les afecten, así como la detección temprana de cualquier incidente que tenga lugar sobre los mismos

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.

### 11.10. Protección de la información almacenada y en tránsito

Se protegerán los entornos que contienen información almacenada y en tránsito entre entornos inseguros tales como equipos o dispositivos portátiles o móviles, dispositivos periféricos, soportes de información y comunicaciones sobre redes abiertas. En este sentido se protegerán convenientemente los equipos portátiles que puedan contener información, así como los soportes extraíbles (pendrives, discos duros extraíbles, etc.) e información en soporte no electrónico.

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.

### 11.11. 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, reforzando las tareas de prevención, detección y respuesta a incidentes de seguridad.

### 11.12. Registro de actividad y detección de código dañino

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, de forma que sea posible impedir el acceso no autorizado a las redes y sistemas de información, detener los ataques de denegación de servicio, evitar la distribución malintencionada de código dañino así como otros daños a las antedichas redes y sistemas de información.




| Código Seguro De Verificación | 654F-3765-4733P3046-5832 | 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 Sustainablity Of The Universidad Complutense de Madrid | Firmado | 01/07/2024 13:07:04 |
| Observaciones | | Página | 20/21 |
| Url De Verificación | https://sede.ucm.es/verificacion?csv=654F-3765-4733P3046-5832 | | |
| Normativa | Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015). | | |

En efecto, se exige a cada usuario tener un identificador único, con sus roles y permisos establecidos, con el objetivo de conocer en todo momento, la trazabilidad de sus acciones.

### 11.13. 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. Se establecerán mecanismos de detección, criterios de clasificación, procedimientos de análisis y resolución. 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.

### 11.14. Continuidad de la actividad

La continuidad de los servicios asociados a las tecnologías de la información se constituyen como un elemento estratégico para la UCM, por ello se disponen de mecanismos técnicos y de gestión para proporcionar acciones de respuesta oportuna ante posibles interrupciones de los servicios, minimizar el tiempo de inactividad y restablecer las actividades a niveles normales de operatividad.

### 11.15. 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 | 654F-3765-4733P3046-5832 | 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 Sustainablity Of The Universidad Complutense de Madrid | Firmado | 01/07/2024 13:07:04 |
| Observaciones | | Página | 21/21 |
| Url De Verificación | https://sede.ucm.es/verificacion?csv=654F-3765-4733P3046-5832 | | |
| Normativa | Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015). | | |