



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

Documentos

UCM Serie:

Seguridad

SE0002 Organización de la Seguridad de la Información

Versión del Documento 3.1

08-03-2024

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.



HOJA DE ESTATUS

Nomenclatura del Documento	Número de versión	Fecha de la versión
SE0002	3.0	
Autores:	USPI	
Distribución:	Comunidad Universitaria	
Resumen:	Directrices de la UCM para la Seguridad de la Información	

HISTORIA DEL DOCUMENTO

Versión	Fecha	Cambios	Autores
1.0	30.09.2014	Documento Inicial	USPI
1.2	03.10.2018	Se incluyen funciones DPD y directrices RGPD	USPI
1.3	24.01.2020	Cambio de formato, actualización de referencias y funciones, reorganización de apartado e inclusión de nuevos diagramas con las funciones.	USPI
2.0	14.02.2022	Adaptación nueva normativa	USPI
3.0	08.03.2024	Actualización de referencias al RD 311/2022	USPI
3.1	24.07.2024	Alineamiento con Política actualizada	USPI



INDICE

1.	ALCANCE	4
2.	DEFINICIONES, ACRÓNIMOS Y ABREVIATURAS	4
3.	REFERENCIAS.....	5
4.	ESTRUCTURA ORGANIZATIVA DE LA SEGURIDAD	6
4.1.	Estructura de especificación	7
4.1.1	Comité de Seguridad de la Información	8
4.1.2	Responsables de la Información	8
4.1.3	Responsables del Servicio	8
4.1.4	El Responsable del Tratamiento	9
4.2.	Estructura de supervisión	10
4.2.1	Comités Técnicos de Seguridad de la Información	10
4.2.2	El Responsable de la Seguridad.....	10
4.2.3	Delegado de Protección de Datos	11
4.3.	Estructura de Operación	13
4.3.1	Responsable del Sistema	13
5.	ANEXO A.....	15



1. ALCANCE

Para poder responder de forma eficaz y eficiente a los retos de la seguridad de la información en la UCM, se deben organizar y estructurar las responsabilidades y las funciones relacionadas con la seguridad, así como asegurar que no existan lagunas.

El objeto de este documento es describir y documentar la estructura de responsabilidades, competencias y relaciones relativas a la seguridad de la información en la UCM.

2. DEFINICIONES, ACRÓNIMOS Y ABREVIATURAS

UCM	Universidad Complutense de Madrid
ENS	Esquema Nacional de Seguridad
RGPD	Reglamento General de Protección de Datos
DPD	Delegado de Protección de Datos
LOPDgdd	Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales
CSI	Comité de Seguridad de la Información
RINFO	Responsable de la Información
RSERV	Responsable del Servicio
RSEG	Responsable de Seguridad
RSIS	Responsable del Sistema
ASS	Administrador de la Seguridad del Sistema
API	Administrador de Protección de la Información
RTRA	Responsable del Tratamiento
DCP	Dato de Carácter Personal



3. 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.
- 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.
- 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).
- 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.

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-201: Organización y gestión para la seguridad de las TIC.
- Guía CCN-STIC-401: Glosario de términos.

4. ESTRUCTURA ORGANIZATIVA DE LA SEGURIDAD

La seguridad en UCM está soportada sobre las estructuras y roles que se describen a continuación:

- **Estructura de especificación**, que es la que se encarga de establecer los requisitos de seguridad asociados a la información y los servicios prestados.
- **Estructura de supervisión**, que es la que se encarga de verificar la correcta implantación y operación de los requisitos de seguridad que se hayan establecido, de cara a mantener la alineación con los objetivos y de cumplir con las normas y legislación aplicable.
- **Estructura de operación**, que se encarga de implantar las medidas de seguridad identificadas.

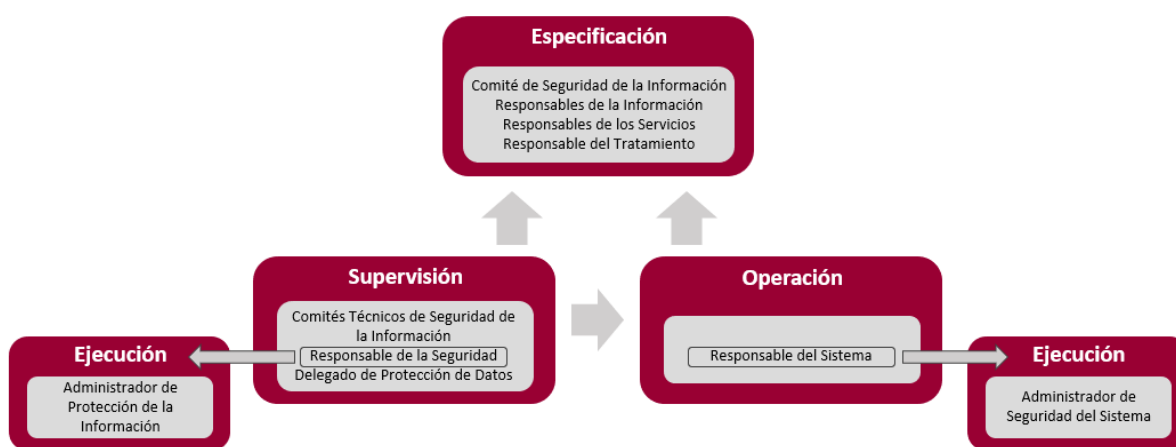


Figura 1. Bloques de responsabilidades

FUNCIONES DELEGADAS



Figura 2. Dependencias

En primer lugar, se crea el **Comité de Seguridad de la Información (CSI)**, quien a su vez creará los **Comités Técnicos de Seguridad de la Información** necesarios para el ágil funcionamiento de una estructura operativa de seguridad, repartida entre las diferentes áreas de responsabilidad de la UCM. El diagrama siguiente representa el esquema de decisión y coordinación de la seguridad de la información.

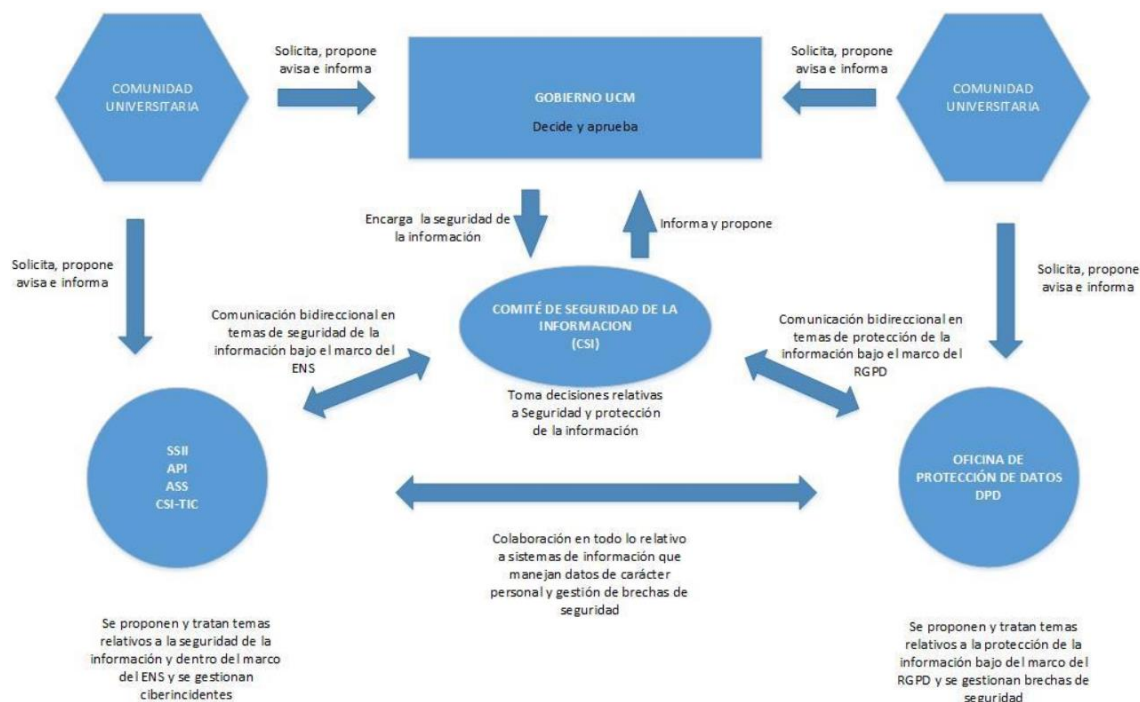


Figura 3. Estructura de la UCM

Con esta estructura se pretende:

- Conseguir decisiones con una coordinación fluida y consistencia en las actuaciones de seguridad: Comité de Seguridad de la Información y Comités Técnicos de Seguridad de la Información.
- Responsabilizar a cada área implicada en la operativa de las medidas de seguridad de su competencia.
- Reportar a los distintos responsables.
- Gestionar los riesgos.
- Crear, comunicar y hacer cumplir la normativa de la UCM en materia de seguridad

4.1. Estructura de especificación

Esta estructura es la encargada de determinar los requisitos de seguridad que se aplicarán a los servicios prestados por UCM y a garantizar el cumplimiento normativo asociado que le es de aplicación, en concreto el texto consolidado del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

Forman parte de esta estructura:

- Comité de Seguridad de la Información.
- Responsables de la Información.
- Responsables de los Servicios.
- Responsable del Tratamiento.



4.1.1 Comité de Seguridad de la Información

El **Comité de Seguridad de la Información (CSI)** tiene como funciones:

- 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 regulador del 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.
- 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 **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.

4.1.2 Responsables de la Información

Las funciones de los responsables de la información son:

- 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.

4.1.3 Responsables del Servicio

Las funciones de los responsables de los servicios son:

- 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.

4.1.4 El Responsable del Tratamiento

Las funciones del responsable del tratamiento son:

- 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.



4.2. Estructura de supervisión

La estructura de supervisión de la seguridad se encarga de verificar la correcta implantación y operación de los requisitos de seguridad que se hayan establecido, de cara a mantener la alineación con los objetivos y de cumplir con las normas y legislación aplicable.

Forman parte de esta estructura:

- Comités Técnicos de Seguridad de la Información.

4.2.1 Comités Técnicos de Seguridad de la Información

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.

4.2.2 El Responsable de la Seguridad

Tiene como responsabilidades mantener la seguridad de la información manejada y de los servicios prestados por los sistemas de información en su ámbito de responsabilidad, de acuerdo con lo establecido en la Política de Seguridad de la UCM.

Las funciones del responsable de la seguridad son:

- 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.
- 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.

4.2.2.1 Administrador de Protección de la Información (API)

Será propuesto por el Responsable de seguridad para nombramiento por el Rector y su ámbito de actuación estará determinado por el alcance del ENS en la UCM.

Las funciones del administrador de protección de la información son:

- La gestión y el análisis de riesgos.
- Asesoramiento en materia de seguridad de la información y protección de datos conforme al Esquema Nacional de Seguridad.
- Incorporar y mantener la documentación de seguridad del sistema.
- Reportar periódicamente al Responsable de la Seguridad y al Responsable del Sistema:
 - Las anomalías, compromisos o vulnerabilidades relacionadas con la seguridad.
 - El cumplimiento de los Procedimientos Operativos de Seguridad.
 - El estado de cumplimiento de los controles de seguridad establecidos conforme a la política de seguridad y análisis de riesgos.
 - Que son aplicados los procedimientos aprobados para manejar los sistemas de información.
- Monitorizar el estado de seguridad de los sistemas con las herramientas disponibles de gestión de eventos de seguridad y mecanismos de auditoría técnica implementados en dichos sistemas.
- Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución.

4.2.3 Delegado de Protección de Datos

Las funciones del delegado de protección de datos son:

- Velar por que la UCM cumpla la normativa de protección de datos (RGPD) 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.
- 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 supervisará 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.

El delegado de protección de datos formará parte del Comité de Seguridad de la Información.



4.3. Estructura de Operación

La estructura de operación de la seguridad debe asumir la administración operativa de la seguridad de los sistemas de información, implantando en dichos sistemas las medidas necesarias para satisfacer los requisitos de seguridad establecidos por la estructura de especificación.

Forman parte de esta estructura:

- El Responsable del Sistema.
- Responsables de la Información.

4.3.1 Responsable del Sistema

Las funciones del responsable del sistema son:

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



4.3.1.1 Administrador de Seguridad del Sistema (ASS)

Será propuesto por el Responsable del Sistema nombramiento por el Rector y su ámbito de actuación estará determinado por el alcance del ENS en la UCM.

Las funciones del administrador de seguridad del sistema son:

- La implementación, gestión y mantenimiento de las medidas de seguridad aplicables a los sistemas de información.
- La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad de los sistemas de información.
- Aprobar los cambios en la configuración vigente de los Sistemas de Información.
- Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida y que en todo momento se ajustan a las autorizaciones pertinentes.
- Informar al Responsable del Sistema y al Administrador de Protección de la Información (API) de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.
- Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución.
- Monitorizar el estado de seguridad de los sistemas con las herramientas disponibles de gestión de eventos de seguridad y mecanismos de auditoría técnica implementados en dichos sistemas.

DELEGACIÓN DE FUNCIONES

- En determinados sistemas de información que, por su complejidad, distribución, separación física de sus elementos o número de usuarios se necesite de personal adicional para llevar a cabo las funciones de ASS, se podrán designar Administradores de Seguridad del Sistema Delegados (ASS-D).
- Los ASS-D serán responsables, en su ámbito, de aquellas acciones que delegue el ASS relacionadas con la implantación, gestión y mantenimiento de las medidas de seguridad aplicables al sistema de información y reportarán cualquier incidencia relacionada con los mismos al ASS.
- El ASS-D será designado por el Responsable del Sistema, a solicitud del ASS del que dependerá funcionalmente. Su identidad aparecerá reflejada en la documentación de seguridad del correspondiente sistema de información.



5. ANEXO A

A continuación, se relacionan resumidas las tareas y sus responsables para los sistemas dentro del ámbito de aplicación del ENS en la UCM. En la tabla se usan las siguientes abreviaturas:

Tarea	Responsable
Determinación de los niveles de seguridad requeridos en cada dimensión	CSI
Determinación de la categoría del sistema	RINFO + RSERV asesora RSEG
Análisis y gestión de riesgos	API
Declaración de aplicabilidad	RSEG
Medidas de seguridad adicionales	RSEG
Configuración de seguridad	Elabora: RSEG Aplica: ASS
Implantación de las medidas de seguridad	ASS
Aceptación del riesgo residual	RINFO + RSERV
Documentación de seguridad del sistema	API
Política de seguridad	Elabora: CSI Aprueba: Rector
Normativa de seguridad	Elabora API Aprueba: CSI
Procedimientos operativos de seguridad	Elabora: RSIS Aprueba: RSEG Aplica: ASS + API
Estado de la seguridad del sistema	RSEG Monitoriza: ASS + API
Planes de mejora de la seguridad	Elaboran: RSIS + RSEG Aprueba: CSI
Planes de concienciación y formación	Elabora: RSEG Aprueba: CSI
Planes de continuidad	Elabora: RSIS Valida: RSEG Coordina y aprueba: CSI Ejercicios: RSIS
Suspensión temporal del servicio	Ejecuta: RSIS Informa a: RSEG + RSERV
Ciclo de vida: especificación, arquitectura, desarrollo, operación, cambios	Elabora: RSIS Aprueba: RSEG
Cumplimiento de la normativa de protección de datos	RTRA Supervisa: DPD