BOLETÍN OFICIAL DE LA UNIVERSIDAD CARLOS III DE MADRID

uc3m | Universidad Carlos III de Madrid

BOEL de 13 de noviembre de 2025

Política de Seguridad de Sistemas de Información basados en Tecnologías de Información y Comunicaciones, aprobado por el Consejo de Gobierno en sesión de 6 de noviembre de 2025

INTRODUCCIÓN

La Universidad Carlos III de Madrid (en adelante Universidad) depende de los sistemas de Información basados en Tecnologías de Información y Comunicaciones (en adelante sistemas TIC) para alcanzar sus objetivos. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad o confidencialidad de la información tratada o los servicios prestados.

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.

Las Leyes 39/2015, del Procedimiento Administrativo Común de las Administraciones Públicas y 40/2015, de Régimen Jurídico del Sector Público, junto con el Real Decreto 3/2010 de 8 de Enero de desarrollo del Esquema Nacional de Seguridad (ENS) establecen los principios básicos y requisitos mínimos que, de acuerdo con el interés general y con la naturaleza y complejidad de la materia regulada, permiten una protección adecuada de la información y los servicios telemáticos.

Es en el Artículo 11 de este Real Decreto 3/2010, modificado por Real Decreto 951/2015, en el que se establece que “todos los órganos superiores de las Administraciones públicas deberán disponer formalmente de su política de seguridad que articule la gestión continuada de la seguridad, que será aprobada por el titular del órgano superior correspondiente”. Con ello se pretende que la seguridad implique a todos los miembros de la organización, que deberán conocer la política de seguridad e identificando unos claros responsables de velar por el cumplimiento de la misma.

Más adelante, el Anexo II del ENS (Medidas de Seguridad; Marco organizativo; Política de seguridad) determina que la política de seguridad se plasmará en un documento escrito, en el que, de forma clara, se precise, al menos los objetivos o misión de la organización, el marco legal y regulatorio en el que se desarrollarán las actividades, los roles o funciones de seguridad, definiendo para cada uno, los deberes y responsabilidades del cargo, así como el procedimiento para su designación y renovación, la estructura del comité o los comités para la gestión y coordinación de la seguridad, detallando su ámbito de responsabilidad, los miembros y la relación con otros elementos de la organización, las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso. Todo ello referenciando y siendo coherente con lo establecido en el Reglamento General de Protección de Datos de la Unión Europea (Reglamento UE 2016/679).

ASPECTOS GENERALES

Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, 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 los diferentes actores implicados deben aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad, 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.

Los diferentes departamentos y servicios deben cerciorarse de que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y las necesidades de financiación, deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos de TIC. Así mismo, deben estar preparados para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo al Artículo 7 del ENS.

Prevención

Los departamentos y servicios deben evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello deben implementar las medidas mínimas de seguridad determinadas por el ENS, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos. Estos controles, y los roles y responsabilidades de seguridad de todo el personal, deben estar claramente definidos, documentados y conocidos por los usuarios de estos sistemas TIC.
Para garantizar el cumplimiento de esta política, los departamentos y servicios deberán:
Autorizar los sistemas antes de entrar en operación.
Evaluar regularmente la seguridad, incluyendo el impacto que supongan los cambios de configuración realizados.
Solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

Detección

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, se deben establecer mecanismos de monitorización continua de la operaciones, para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia según lo establecido en el Artículo 9 del ENS.
La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el Artículo 8 del ENS. Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales.

Respuesta

Los diferentes departamentos y servicios deben:
Establecer mecanismos para responder eficazmente a los incidentes de seguridad.

Designar punto de contacto para las comunicaciones con respecto a incidentes detectados.
Establecer protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT).

Recuperación

Para garantizar la disponibilidad de los servicios críticos, los departamentos y servicios deben desarrollar planes de continuidad de los sistemas TIC como parte de su plan general de continuidad de servicio y actividades de recuperación.

ALCANCE

Es objeto de la presente Política de Seguridad plasmar en un documento escrito, el conjunto de directrices que rigen la forma en la que la Universidad, gestiona y protege los recursos de información y los sistemas que considera críticos para permitir el ejercicio de derechos y el cumplimiento de deberes por medios electrónicos en cumplimiento de lo establecido en la Ley 11/2007 de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos.
Esta política se aplica a todos los sistemas TIC de la Universidad y a todas aquellas personas, instituciones, entidades, departamentos y servicios que hagan uso de ellos, sin excepciones.
En este sentido, serán considerados sistemas TIC de la Universidad todos aquellos sistemas que emplean tecnologías de la información y de las comunicaciones para recoger, almacenar, procesar o tratar, mantener, usar, compartir, distribuir, poner a disposición, presentar o transmitir datos e información.
Por el contrario, no se considerará sistema TIC de la Universidad a aquellos ordenadores personales financiados a título individual, no inventariados a nombre de la universidad, aunque pudieran ocasionalmente ser usados para labores propias de investigación. Por tanto quedan fuera de este ámbito dichos elementos. En estos casos, la Universidad se reserva el derecho de proporcionar acceso a la red de este tipo de recursos ajenos a la misma si no se proporcionan unos mínimos requisitos de seguridad o existan indicios o

evidencias de un incidente potencial de seguridad que pueda comprometer o bien la seguridad de la información de los sistemas TIC o bien su buen nombre o imagen corporativa.

MISIÓN

La misión de la Universidad Carlos III de Madrid es ofrecer un servicio público de educación superior de calidad, de prestigio nacional e internacional, a través de una formación integral centrada en el estudiantado y una investigación de vanguardia que contribuya, mediante la generación y transferencia de conocimiento, al desarrollo económico y a la transformación de la sociedad.

La Universidad ejerce las potestades y ostenta las prerrogativas que el ordenamiento jurídico le reconoce en su calidad de Administración pública, desempeñando las siguientes funciones:

Fomentará la calidad y excelencia en sus actividades, estableciendo sistemas de control y evaluación, que podrán ser obligatorios para los miembros de la comunidad universitaria.

Velará por el adecuado desarrollo de la docencia para la transmisión y crítica de la ciencia, de la técnica y de la cultura.

Apoyará la investigación como procedimiento de creación y renovación del conocimiento.

Prestará una atención especial a los estudios de Postgrado (Máster y Doctorado) en general y en particular a la formación de doctores.

Establecerá relaciones con otras Universidades, centros de educación superior y centros de investigación.

Procurará la mayor proyección social de sus actividades, mediante el establecimiento de cauces de colaboración y asistencia a la sociedad, con el fin de apoyar el progreso social, económico y cultural.

Apoyará la cooperación universitaria al desarrollo a través de estrategias orientadas a la transformación social y el fortalecimiento académico en los países más desfavorecidos.

Garantizará la igualdad de trato y de oportunidades de todas las personas, procurando una presencia equilibrada de hombres y mujeres en todos sus órganos de decisión.

En la realización de sus actividades, la Universidad se atendrá a los principios de legalidad, eficacia, eficiencia, transparencia, calidad, igualdad y mejor servicio a la sociedad y a los miembros de la comunidad universitaria.

MARCO NORMATIVO

La Universidad Carlos III de Madrid mantendrá un registro de la normativa aplicable a esta Política, públicamente disponible en la siguiente dirección https://docs.google.com/document/d/135h_7BcKo7jEbnoOVbcyxCbVSrvFapjkj5zYhRD8Ef4

ORGANIZACIÓN DE LA SEGURIDAD

El mantenimiento y gestión de la Seguridad de los Sistemas de Información depende íntimamente del establecimiento de una Organización de la Seguridad. Dicha Organización queda establecida mediante la identificación y definición de las diferentes actividades y responsabilidades en materia de gestión de la Seguridad así como de la implantación de una estructura que las soporte. A continuación se describen las estructuras establecidas en la Universidad Carlos III de Madrid con responsabilidad en diversas áreas relacionadas con la Gestión de la Seguridad de la Información.

COMITÉS: funciones y responsabilidades

Consejo Informático

El Consejo Informático es el órgano colegiado de participación en la planificación, desarrollo y gestión de los recursos informáticos de la Universidad.

Su composición y funciones se definen en el artículo 4 del Reglamento de Organización y Funcionamiento del Servicio de Informática, aprobado por Acuerdo de la Junta de Gobierno, en su sesión 3/97, de 17 de junio de 1.997.

Composición

- Presidente: el Rector o, en su caso, Vicerrector competente por razón de la materia, de acuerdo con lo previsto en el artículo anterior.
- Vocales: El Gerente de la Universidad.

- Los Decanos y Directores de Escuela Politécnica Superior, o Vicedecanos o Subdirectores en quienes éstos deleguen.
- Un representante de cada uno de los Departamentos de la Universidad.
- Un representante de los Institutos Universitarios por cada uno de los Campus en los que se organiza la Universidad.
- Un representante de los alumnos de cada una de las Facultades o Escuelas Politécnicas Superiores.
- Un representante de los Servicios de la Universidad nombrado por el Rector.
- Un representante del personal de administración y servicios del Servicio de Informática.
- Secretario: el Director del Servicio de Informática y Comunicaciones

Funciones

El Consejo Informático tendrá la función de informar sobre:

- La aprobación de las disposiciones que afecten al Servicio de Informática.
- Los requisitos para la integración de recursos informáticos en el Sistema General de Informática de la Universidad
- Los planes, normas técnicas y catálogos relativos a los servicios de seguridad informática de la Universidad, de tratamiento automatizado de datos, o prestaciones garantizadas por el Servicio de Informática de la Universidad.
- De conocimiento y, en su caso, informe sobre las decisiones de los órganos de gobierno de la Universidad que afecten al Servicio de Informática para los que sea recabada la consulta de éste.

Comisión de Administración Electrónica

La Comisión de Administración Electrónica de la Universidad Carlos III de Madrid se configura como órgano asesor del Rector y del Consejo de Dirección en materia de Administración Electrónica.

Su composición y funciones quedan determinadas en el artículo 6 (Comisión de Administración Electrónica) del Título II del Reglamento por el que se crea la Sede Electrónica de la Universidad Carlos III de Madrid y se establecen las condiciones básicas de acceso de los ciudadanos a los servicios de la Universidad, aprobado por el Consejo de

Gobierno de la Universidad en sesión de 9 de diciembre de 2010 y publicado en el Boletín Oficial de la Comunidad de Madrid (BOCM) del viernes 14 de enero de 2011.

Composición

La composición de la Comisión de Administración Electrónica estará recogida en la normativa de la Sede Electrónica de la Universidad Carlos III de Madrid.

Adicionalmente podrá invitar a sus reuniones, cuando sea preciso, a Profesores e Investigadores especialistas en la materia, a otros Directores de Servicios y Unidades Administrativas de la Universidad, así como cualquier otra persona que considere conveniente para el desarrollo de sus funciones.

Funciones

La Comisión de Administración Electrónica tiene como funciones principales impulsar la implantación de la Administración Digital/Electrónica en la Universidad, asesorar al Rector y al Consejo de Dirección, así como velar por el cumplimiento de obligaciones, principios y derechos recogidos en la normativa de aplicación.

Comisión de Protección de Datos

La comisión de Protección de Datos es el órgano de la Universidad encargado del cumplimiento de la legislación vigente en materia de Protección de Datos de Carácter Personal. Su composición y funciones se detallan a continuación.

Composición

- Secretaría General, que la presidirá.
- Cargo institucional competente en materia de tecnologías de la información.
- Gerencia.
- Delegado de Protección de Datos (DPD), que actuará como secretario.
- Responsable de Seguridad de la Información (CISO, Chief Information Security Officer).
- Vicegerencia o Dirección con competencia en materia de estudios en la Universidad.
- Dirección del Servicio de Recursos Humanos y Organización.
- Dirección del Servicio Jurídico.
- Dirección del Servicio de Informática y Comunicaciones.

- Responsable de la gestión de datos en la Universidad.
- Expertos en Protección de Datos

Adicionalmente podrá invitar a sus reuniones, cuando sea preciso, a Profesores e Investigadores especialistas en la materia, a otros Directores de Servicios y Unidades Administrativas de la Universidad, así como cualquier otra persona que considere conveniente para el desarrollo de sus funciones.

Funciones

La Comisión de Protección de Datos tiene como objetivos principales:

- Velar por el cumplimiento de la normativa de protección de datos y controlar su aplicación.
- Impulsar y controlar la implantación de medidas relacionadas con el cumplimiento de la normativa de Protección de Datos.
- Evaluación de la situación de la protección de datos y seguridad informática en la Universidad Carlos III de Madrid.
- Proponer recomendaciones y acciones en materia de protección de datos y seguridad informática.
- Informar en sus ámbitos de actuación.
- Colaboración con el Consejo Informático.
- Recibir información del Delegado de Protección de Datos sobre la actividad desarrollada por éste y el cumplimiento normativo de protección de datos por la Universidad.
- Aprobar documentación en forma de guías e instrucciones, recomendaciones, orientada a facilitar por parte de la comunidad universitaria el cumplimiento normativo en materia de protección de datos personales.

Comisión de Seguridad de la Información

Composición

- Cargo institucional competente en materia de tecnologías de la información, que la presidirá.
- Secretaría General.
- Gerencia.

- Delegado de Protección de Datos (DPD).
- Responsable de Seguridad de la Información (CISO, Chief Information Security Officer), que actuará como secretario.
- Vicegerencia o Dirección con competencia en materia de estudios en la Universidad.
- Dirección del Servicio de Recursos Humanos y Organización.
- Dirección del Servicio Jurídico.
- Dirección del Servicio de Informática y Comunicaciones.
- Responsable de la gestión de datos en la Universidad.
- Expertos en Seguridad de la Información.

Adicionalmente podrá invitar a sus reuniones, cuando sea preciso, a Profesores e Investigadores especialistas en la materia, a otros Directores de Servicios y Unidades Administrativas de la Universidad, así como cualquier otra persona que considere conveniente para el desarrollo de sus funciones.

Funciones

El Comité de Seguridad de la Información coordina la seguridad de la información a nivel de organización, con las siguientes funciones y responsabilidades:

- Elaborar la estrategia de evolución de la Organización en lo que respecta a seguridad de la información.
- Atender las inquietudes de los Órganos de Gobierno y de los diferentes Departamentos en materia de Seguridad de la Información.
- Informar regularmente del estado de la seguridad de la información a los Órganos de Gobierno.
- Promover la mejora continua del sistema de gestión de la seguridad de la información.
- Coordinar los esfuerzos de los diferentes departamentos y servicios en materia de seguridad de la información, para asegurar que los esfuerzos son consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades.
- Elaborar (y revisar regularmente) la Política de Seguridad de la información para que sea aprobada por los Órganos de Gobierno.

- Elaborar (y revisar regularmente) la normativa de seguridad de la información, para que sea aprobada por los Órganos de Gobierno.
- Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios desde el punto de vista de seguridad de la información, en coherencia con la normativa vigente.
- Monitorizar los principales riesgos residuales asumidos por la Organización y recomendar posibles actuaciones respecto de ellos.
- Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones respecto de ellos. En particular, velar por la coordinación de las diferentes áreas de seguridad en la gestión de incidentes de seguridad de la información.
- Promover la realización de auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad.
- Elaborar planes de mejora de la seguridad de la información de la Organización, para que sean aprobados por los Órganos de Gobierno. En particular velará por la coordinación de diferentes planes que puedan realizarse en diferentes áreas.
- Priorizar las actuaciones en materia de seguridad cuando los recursos sean limitados.
- Velar porque la seguridad de la información se tenga en cuenta en todos los proyectos TIC 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 TIC.
- Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables y/o entre diferentes áreas de la Organización, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.

ROLES: funciones y responsabilidades

El artículo 10 del ENS (la seguridad como función diferenciada) establece que en los sistemas de información se diferenciarán tres responsables:

- Responsable de la Información

- Responsable del Servicio
- Responsable de la Seguridad

El Responsable de la Información determinará los requisitos de la información tratada; el Responsable del Servicio determinará los requisitos de los servicios prestados; y el Responsable de Seguridad determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios, debiendo estar la responsabilidad de la seguridad de los sistemas de información diferenciada de la responsabilidad sobre la prestación de los mismos.

Responsable de la Información

El ENS asigna al Responsable de la Información la potestad de determinar los niveles de seguridad de la misma (Art. 44), siendo habitual su ocupación por un alto cargo en la dirección, que entiende la misión de la organización, determina los objetivos que se propone alcanzar y responde de que se alcancen.

La figura del Responsable de la Información recaerá en el Gerente de la Universidad.

Serán sus funciones y responsabilidades:

- Responsabilidad última del uso que se haga de una cierta información y, por tanto, de su protección, es el responsable último de cualquier error o negligencia que lleve a un incidente de confidencialidad o de integridad.
- Potestad de establecer los requisitos de la información en materia de seguridad, es decir, potestad para determinar los niveles requeridos en cada dimensión de seguridad.

Aunque la aprobación formal de los niveles corresponda al Responsable de la Información, se puede recabar una propuesta al Responsable de la Seguridad y se escuchará la opinión del Responsable del Sistema.

Responsable del Servicio

El Responsable del Servicio tiene la potestad de establecer los requisitos del servicio en materia de seguridad, es decir, según define el artículo 44 del ENS, la potestad de determinar los niveles de seguridad de los servicios.

La responsabilidad del servicio será ejercida por el director de cada servicio en los que se estructura la universidad.

Serán sus funciones y responsabilidades:

- Responsabilidad última del uso que se haga de un cierto servicio y, por tanto, de su protección, es el responsable último de cualquier error o negligencia que lleve a un incidente de disponibilidad.
- Potestad de establecer los requisitos del servicio en materia de seguridad, es decir, potestad para determinar los niveles requeridos en cada dimensión de seguridad.

Aunque la aprobación formal de los niveles corresponda al Responsable del Servicio, se puede recabar una propuesta al Responsable de la Seguridad y se escuchará la opinión del Responsable de los Sistemas de Información.

Responsable de los Sistemas de Información

La figura de Responsable de los Sistemas de Información recaerá en la Dirección del Servicio de Informática y Comunicaciones. Serán suyas las siguientes funciones y responsabilidades:

- Desarrollar, operar y mantener el Sistema de Información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.
- Definir la topología y sistema de gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.
- Podrá acordar la suspensión del manejo de una cierta información o la prestación de un cierto servicio si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. Esta decisión debe ser acordada con los responsables de la información afectada, del servicio afectado y el Responsable de la Seguridad, antes de ser ejecutada.
- Elaborar los procedimientos operativos de seguridad, los planes de mejora de la seguridad y los planes de continuidad.
- Informar y servir de nexo de unión con los consejos y comisiones relacionados.

Responsable de Seguridad

El Responsable de la Seguridad determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.

El Responsable de Seguridad será determinado por la Dirección del Servicio de Informática y Comunicaciones, siendo sus funciones y responsabilidades:las que se detallan a continuación:

- Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas de información en su ámbito de responsabilidad, de acuerdo a lo establecido en esta Política de Seguridad de la Organización.
- Promover la formación y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad.
- Determinar la categoría de los sistemas y las medidas de seguridad que deben aplicarse según procedimientos descritos en los Anexos I y II del ENS.
- Validar los procedimientos operativos de seguridad, los planes de mejora de la seguridad y los planes de continuidad.
- Analizar y proponer salvaguardas que prevengan incidentes de seguridad.
- Realizar o instar a la realización de un análisis de riesgos con revisión y aprobación bienal.
- Realizar o instar a la realización de auditorías periódicas.
- Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica implementados en los sistemas.
- Elaborar la Normativa de Seguridad.

Administrador del Sistema (AS)

El Administrador del Sistema es responsable de la implantación, gestión y mantenimiento de las medidas de seguridad aplicables al Sistema y de la redacción de los Procedimientos Operativos de Seguridad.

Serán sus funciones y responsabilidades:

- La implementación, gestión y mantenimiento de las medidas de seguridad aplicables al Sistema 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 del Sistema de Información.

- La gestión de las autorizaciones concedidas a los usuarios del sistema, en particular los privilegios concedidos, incluyendo la monitorización de que la actividad desarrollada en el sistema se ajusta a lo autorizado.
- La aplicación de los Procedimientos Operativos de Seguridad.
- Definir los cambios en la configuración vigente del Sistema de Información.
- Asegurar que los controles de seguridad establecidos son cumplidos estrictamente.
- Asegurar que son aplicados los procedimientos aprobados para manejar el sistema de información.
- Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida y que en todo momento se ajustan a las autorizaciones pertinentes.
- Informar a los Responsables de la Seguridad y de los Sistemas de Información 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.

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La presente Política de Seguridad será aprobada por el Consejo de Gobierno, siendo responsabilidad del Comité de Seguridad TIC su revisión anual y la propuesta de actualización o mantenimiento de la misma cuando sea necesario.
La información de difusión pública se alojará en la Sede Electrónica de la Universidad Carlos III de Madrid, en la dirección https://www.uc3m.gob.es.
Esta Política de Seguridad de la Información será efectiva desde el momento de su aprobación y hasta que sea reemplazada por una nueva Política.

DATOS DE CARÁCTER PERSONAL

La Universidad Carlos III de Madrid trata datos de carácter personal. Los documentos de seguridad, a los que tendrán acceso sólo las personas autorizadas, recogen los ficheros afectados y los responsables correspondientes. Todos los sistemas de información de UC3M se ajustarán a los niveles de seguridad requeridos por la normativa para la naturaleza y finalidad de los datos de carácter personal recogidos en el mencionado Documento de Seguridad, que recoge todas las medidas técnicas y organizativas que se han implantado para garantizar la seguridad de los datos, los sistemas y las personas que intervienen en el tratamiento de los mismos.
Es misión de la Comisión LOPD, vigilar el cumplimiento de este apartado.

GESTIÓN DE RIESGOS

Todos los sistemas sujetos a esta Política deberán realizar un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos, así como proponiendo las medidas adecuadas para contrarrestar o mitigar el riesgo. Este análisis se repetirá:

- Regularmente, al menos una vez al año
- Cuando cambie la información manejada
- Cuando cambien los servicios prestados
- Cuando ocurra un incidente grave de seguridad
- Cuando se reporten vulnerabilidades graves

Para la armonización de los análisis de riesgos, el Comité de Seguridad TIC establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados. El Comité de Seguridad TIC dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

DESARROLLO DE LA POLÍTICA DE SEGURIDAD

Esta Política de Seguridad de la Información complementa los reglamentos, políticas y procedimientos de seguridad existentes actualmente en la UC3M para diferentes materias:

- Reglamento del Servicio de Informática y Comunicaciones

Reglamento de Organización y Funcionamiento del Servicio de Informática, aprobado por Acuerdo de la Junta de Gobierno, en su sesión 3/97, de 17 de junio de 1.997

- Reglamento de Aulas Informáticas

Aprobado en Consejo Informático de Junio de 1993

- Reglamento Delegación de Zona del Dominio UC3M

Aprobado en Consejo Informático de 15 de Febrero de 2007.

- Política de Instalación de Puntos de Acceso Inalámbricos

Aprobado en Consejo Informático de Marzo de 2004

- Protocolo de desconexión de equipos de la red de datos por motivos de seguridad

Aprobado en Consejo Informático de Marzo de 2004

- Protocolo de bloqueo de cuentas comprometidas

Aprobado en Consejo Informático del 19 de Marzo de 2013

- Reputación Web

Aprobado en Consejo Informático del 19 de Marzo de 2013

Esta Política se desarrollará por medio de una Normativa de Seguridad que afronte aspectos específicos. La Normativa de Seguridad estará a disposición de todos los miembros de la organización que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

OBLIGACIONES DEL PERSONAL

Todos los miembros de la Universidad Carlos III de Madrid tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad, siendo responsabilidad del Comité de Seguridad TIC proporcionar los medios necesarios para que la información llegue a los afectados.

Todos los miembros de la UC3M, dispondrán de materiales informativos para mejorar su concienciación en materia de seguridad TIC. Se establecerá un programa de concienciación continua para atender a todos los miembros, en particular a los de nueva incorporación, con la obligación de participación con la periodicidad que apruebe la Comisión de Seguridad de la Información.

Las personas con responsabilidad en el uso, operación o administración de sistemas TIC recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo. La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

En el caso de detectarse incumplimiento de las medidas contempladas en esta Política de Seguridad o en sus normativas de desarrollo, se podrán aplicar medidas preventivas y correctoras, encaminadas a proteger los sistemas TIC. El procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario del personal al servicio de las Administraciones Públicas o de la propia Universidad Carlos III de Madrid.

TERCERAS PARTES

Cuando la Universidad Carlos III de Madrid preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipes de esta Política de Seguridad, estableciéndose canales para reporte y coordinación así como procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando la UC3M utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad y de la Normativa de Seguridad que ataña a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias. Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política.

Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por los responsables de la información y los servicios afectados antes de seguir adelante.

ANEXO I: HERRAMIENTAS PARA IMPLEMENTAR LA POLÍTICA

Dado que esta Política de Seguridad está escrita a un nivel muy amplio, se requiere complementarla con documentos más precisos que ayuden a llevar a cabo lo propuesto. Para ello se utilizan otros instrumentos que reciben diferentes nombres, siendo comunes los siguientes:

- Normas de seguridad: Dan uniformidad al uso de aspectos concretos del sistema. Indican el uso correcto y las responsabilidades de los usuarios. Son de carácter obligatorio.
- Guías de seguridad: tienen un carácter formativo y buscan ayudar a los usuarios a aplicar correctamente las medidas de seguridad proporcionando razonamientos donde no existen procedimientos precisos. Ayudan a prevenir que se pasen por alto aspectos importantes de seguridad.
- Procedimientos de seguridad: Afrontan tareas concretas, indicando lo que hay que hacer, paso a paso. Son útiles en tareas repetitivas

ANEXO II: GLOSARIO

- Análisis de riesgos: Utilización sistemática de la información disponible para identificar peligros y estimar los riesgos.
- Autenticidad: Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.
- Confidencialidad: Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados.
- Datos de carácter personal: Cualquier información concerniente a personas físicas identificadas o identificables; se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona (Reglamento UE 2016/679, Reglamento General de Protección de Datos).
- Gestión de incidentes: Plan de acción para atender a las incidencias que se den. Además de resolverlas debe incorporar medidas de desempeño que permitan conocer la calidad del sistema de protección y detectar tendencias antes de que se conviertan en grandes problemas.
- Gestión de riesgos: Actividades coordinadas para dirigir y controlar una organización con respecto a los riesgos.
- Incidente de seguridad: Suceso inesperado o no deseado con consecuencias en detrimento de la seguridad del sistema de información.
- Integridad: Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada.
- Política de seguridad: Conjunto de directrices plasmadas en documento escrito, que rigen la forma en que una organización gestiona y protege la información y los servicios que considera críticos.
- Principios básicos de seguridad: Fundamentos que deben regir toda acción orientada a asegurar la información y los servicios.

- Responsable de la información: Persona que tiene la potestad de establecer los requisitos de una información en materia de seguridad.
- Responsable de la seguridad: El responsable de seguridad determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.
- Responsable del servicio: Persona que tiene la potestad de establecer los requisitos de un servicio en materia de seguridad.
- Responsable del sistema: Persona que se encarga de la explotación del sistema de información.
- Servicio: Función o prestación desempeñada por alguna entidad oficial destinada a cuidar intereses o satisfacer necesidades de los ciudadanos.
- Sistema de información: Conjunto organizado de recursos para que la información se pueda recoger, almacenar, procesar o tratar, mantener, usar, compartir, distribuir, poner a disposición, presentar o transmitir.
- Sistema TIC: Sistema de información que emplea tecnologías de la información y de las comunicaciones.
- Trazabilidad: Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad.

ANEXO III. BIBLIOGRAFÍA

- GUÍA DE SEGURIDAD (CCN-STIC-806). ESQUEMA NACIONAL DE SEGURIDAD: PLAN DE ADECUACIÓN.
- GUÍA DE SEGURIDAD (CCN-STIC-804) ESQUEMA NACIONAL DE SEGURIDAD: GUÍA DE IMPLANTACIÓN (BORRADOR).
- GUÍA DE SEGURIDAD (CCN-STIC-815). ESQUEMA NACIONAL DE SEGURIDAD: MÉTRICAS E INDICADORES.
- GUÍA DE SEGURIDAD (CCN-STIC-808). VERIFICACIÓN DEL CUMPLIMIENTO DE LAS MEDIDAS EN EL ENS.
- GUÍA DE SEGURIDAD (CCN-STIC-804). ESQUEMA NACIONAL DE SEGURIDAD GUÍA DE IMPLANTACIÓN (BORRADOR).
- GUÍA DE SEGURIDAD (CCN-STIC-803). ESQUEMA NACIONAL DE SEGURIDAD VALORACIÓN DE LOS SISTEMAS.
- GUÍA DE SEGURIDAD (CCN-STIC-801) ESQUEMA NACIONAL DE SEGURIDAD RESPONSABILIDADES Y FUNCIONES
- GUÍA DE SEGURIDAD (CCN-STIC-801) ESQUEMA NACIONAL DE SEGURIDAD RESPONSABILIDADES Y FUNCIONES
- MAGERIT v.3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Ministerio de Hacienda y Administraciones Públicas, octubre 2012
- http://www.pilar-tools.com/es/tools/pilar_basic/v52/help_basic_es_e_2012-07-20.pdf
- NIST SP 800-100, An Introduction to Computer Security: The NIST Handbook, October 1995.