Política de Seguridad de la Información de la Universidad de Castilla-La Mancha

Índice

1. Introducción

La Universidad de Castilla-La Mancha considera la información un elemento fundamental para el cumplimiento de su misión y los valores y principios que la inspiran. Por ello, se ha marcado la responsabilidad de protegerla a través de la Política de Seguridad de la Información que se define en este documento, donde se establecen unas directrices básicas de acuerdo a los requisitos propios de seguridad y a la regulación aplicable.

El sistema de Tecnologías de Información y Comunicaciones (TIC) del que hace uso la Universidad para alcanzar sus objetivos debe ser administrado con diligencia, tomando las medidas adecuadas para protegerlo 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 confidencialidad, integridad y autenticidad de la información, así como la disponibilidad de los servicios que presta la Universidad, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.

Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución que puedan 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 se 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.

La Universidad de Castilla-La Mancha debe 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.

La Universidad de Castilla-La Mancha debe estar preparada para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo al artículo 8 del *Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad*, por lo que esta Política establece medidas organizativas y técnicas que permitan garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria para detectar cualquier incidente y reaccionando con presteza a los incidentes para recuperar los servicios lo antes posible.

2. Objeto del documento

El presente documento tiene por objeto definir la Política de Seguridad de la Información de la Universidad de Castilla-La Mancha. Con esta Política se pretende garantizar a los miembros de la comunidad universitaria y a los ciudadanos que el ejercicio de sus derechos y obligaciones se realice de forma segura y conforme a la legislación vigente.

2.1. Prevención

La Universidad de Castilla-La Mancha debe 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 se implementarán las medidas de seguridad determinadas por el Esquena Nacional de Seguridad (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, estarán definidos y documentados.

Para garantizar el cumplimiento de esta Política, de manera preventiva, se deberá:

- Autorizar los sistemas antes de entrar en operación.
- Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
- Solicitar la revisión periódica por parte de terceros, con el fin de obtener una evaluación independiente. Esta revisión se realizará como máximo cada dos años mediante auditorías externas a la Universidad.

2.2. Detección

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su parada, se monitorizarán las operaciones de manera continuada para detectar anomalías en los niveles de prestación de los mismos y se actuará en consecuencia según lo establecido en el artículo 10 del ENS, reevaluando y actualizando periódicamente las medidas de seguridad para adecuarlas a la evolución de los riesgos y los sistemas de protección.

La monitorización es especialmente relevante en el supuesto de que se establezcan líneas de defensa de acuerdo con el artículo 9 del ENS. Los mecanismos de detección, análisis y reporte llegarán a los responsables de la Información y los Servicios, de la Seguridad y del Sistema regularmente y cuando se produzca una desviación significativa de los parámetros que se hayan preestablecido como normales.

2.3. Respuesta

Se deberá:

- Establecer mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar un punto de contacto para las comunicaciones con respecto a incidentes detectados en otras administraciones públicas u otros organismos.
- Establecer protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT).

2.4. Recuperación

Para garantizar la disponibilidad de los servicios críticos, se desarrollará planes de continuidad de los sistemas TIC como parte del plan general de continuidad de negocio y actividades de recuperación.

3. Misión de la Organización

La misión de la Universidad de Castilla-La Mancha es la prestación del servicio público de la educación superior, mediante la docencia y el estudio, la investigación, la transferencia de conocimiento a la sociedad, la difusión de la cultura y la extensión universitaria, con autonomía respecto de cualquier poder económico, social, ideológico o político.

Son sus fines:

a) La creación, desarrollo y crítica de la ciencia, de la técnica y de la cultura a través del estudio y la investigación.
b) La transmisión crítica del conocimiento científico, técnico y cultural por medio de la educación de nivel superior, mediante una actividad docente y formativa de calidad.
c) La preparación para el ejercicio de actividades profesionales que exijan la aplicación de conocimientos y métodos científicos y para la creación artística.
d) La difusión del saber universitario en la sociedad, así como la recepción de las manifestaciones culturales producidas en su entorno.

e) El apoyo científico y técnico al desarrollo cultural, social y económico, con atención singular a las demandas particulares de la Comunidad Autónoma de Castilla-La Mancha en cuyo ámbito territorial está ubicada.

4. Principios básicos

Los principios básicos son directrices fundamentales de seguridad que han de tenerse siempre presentes en cualquier actividad relacionada con el uso de los activos de información. Se establecen los siguientes:

- **Alcance estratégico**: La seguridad de la información debe contar con el compromiso y apoyo de todos los niveles directivos de la universidad, de forma que pueda estar coordinada e integrada con el resto de las iniciativas estratégicas de la organización para conformar un todo coherente y eficaz.
- **Responsabilidad determinada**: En los sistemas TIC se determinará el Responsable de la Información, que determina los requisitos de seguridad de la información tratada; el Responsable del Servicio, que determina los requisitos de seguridad de los servicios prestados; el Responsable del Sistema, que tiene la responsabilidad sobre la prestación de los servicios y el Responsable de la Seguridad, que determina las decisiones para satisfacer los requisitos de seguridad.
- **Seguridad integral**: La seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con los sistemas TIC, procurando evitar cualquier actuación puntual o tratamiento coyuntural. La seguridad de la información debe considerarse como parte de la operativa habitual, estando presente y aplicándose desde el diseño inicial de los sistemas TIC.
- **Gestión de Riesgos**: El análisis y gestión de riesgos será parte esencial del proceso de seguridad. La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, el impacto y la probabilidad de los riesgos a los que estén expuestos y la eficacia y el coste de las medidas de seguridad. Al evaluar el riesgo en relación con la seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales.
- **Proporcionalidad**: El establecimiento de medidas de protección, detección y recuperación deberá ser proporcional a los potenciales riesgos y a la criticidad y valor de la información y de los servicios afectados.
- **Mejora continua**: Las medidas de seguridad se reevaluarán y actualizarán periódicamente para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección. La seguridad de la información será atendida, revisada y auditada por personal cualificado, instruido y dedicado.

5. Objetivos de la Seguridad de la Información

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

- **Garantizar la calidad y protección de la información**.
- Lograr la plena **concienciación de los usuarios** respecto a la seguridad de la información.
- **Gestión de activos de información**: Los activos de información de la Universidad se encontrarán inventariados y categorizados y estarán asociados a un responsable.
- **Seguridad ligada a las personas**: Se implantarán los mecanismos necesarios para que cualquier persona que acceda, o pueda acceder a los activos de información, conozca sus responsabilidades y de este modo se reduzca el riesgo derivado de un uso indebido, logrando la plena concienciación de los usuarios respecto a la seguridad de la información.

- **Seguridad física**: Los activos de información serán emplazados en áreas seguras, protegidas por controles de acceso físicos adecuados a su nivel de criticidad. Los sistemas y los activos de información que contienen dichas áreas estarán suficientemente protegidos frente a amenazas físicas o ambientales.
- **Seguridad en la gestión de comunicaciones y operaciones**: Se establecerán los procedimientos necesarios para lograr una adecuada gestión de la seguridad, operación y actualización de las TIC. La información que se transmita a través de redes de comunicaciones deberá ser adecuadamente protegida, teniendo en cuenta su nivel de sensibilidad y de criticidad, mediante mecanismos que garanticen su seguridad.
- **Control de acceso**: Se limitará el acceso a los activos de información por parte de usuarios, procesos y otros sistemas de información mediante la implantación de los mecanismos de identificación, autenticación y autorización acordes a la criticidad de cada activo. Además, quedará registrada la utilización del sistema con objeto de asegurar la trazabilidad del acceso y auditar su uso adecuado, conforme a la actividad de la organización.
- **Adquisición, desarrollo y mantenimiento de los sistemas de información**: Se contemplarán los aspectos de seguridad de la información en todas las fases del ciclo de vida de los sistemas de información, garantizando su seguridad por defecto.
- **Gestión de los incidentes de seguridad**: Se implantarán los mecanismos apropiados para la correcta identificación, registro y resolución de los incidentes de seguridad.
- **Garantizar la prestación continuada de los servicios**: Se implantarán los mecanismos apropiados para asegurar la disponibilidad de los sistemas de información y mantener la continuidad de los servicios, de acuerdo a los niveles de criticidad de estos.
- **Protección de los datos**: Se adoptarán las medidas técnicas y organizativas que corresponda implantar para atender los riesgos generados por el tratamiento para cumplir la legislación de seguridad y privacidad.
- **Cumplimiento**: Se adoptarán las medidas técnicas, organizativas y procedimentales necesarias para el cumplimiento de la normativa legal vigente en materia de seguridad de la información.

6. Ámbito de aplicación

La presente Política de Seguridad de la Información se aplicará a los sistemas de información de la Universidad de Castilla-La Mancha relacionados con el ejercicio de sus competencias y, en concreto, con los que soporten los siguientes servicios:

- Soporte a la Docencia
- Soporte a la Investigación
- Soporte a la Gestión
- Correo y colaboración
- Publicación web de contenidos
- Comunicaciones
- Administración electrónica

Esta Política también será de aplicación a todos los usuarios con acceso autorizado a los sistemas de información, sean o no empleados públicos y con independencia de la naturaleza de su relación jurídica con la Universidad. Todos ellos tienen la obligación de conocerla y cumplirla, así como las normas de seguridad que de ella se deriven, siendo responsabilidad del Comité de Ciberseguridad disponer los medios necesarios para que la información llegue al personal afectado.

7. Marco normativo

El marco normativo en que desarrolla sus actividades la Universidad de Castilla-La Mancha está constituido, principalmente, por las siguientes normas:

- Ley Orgánica 2/2023, de 22 de marzo, del Sistema Universitario.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).
- Ley 27/1982, de 30 de junio, sobre creación de la Universidad Castellano-Manchega.
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- Ley 56/2007, de 28 de diciembre, de medidas de impulso de la Sociedad de la Información.
- Ley 14/2011, de 1 de junio, de la Ciencia, la Tecnología y la Innovación.
- Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.
- Ley 11/2022, de 28 de junio, General de Telecomunicaciones.
- 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 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014.
- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
- Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones.
- Real Decreto 1553/2005, de 23 de diciembre, por el que se regula el documento nacional de identidad y sus certificados de firma electrónica.
- 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.
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Resolución de 18/11/2015, de la Dirección General de Universidades, Investigación e Innovación, por la que se ordena la publicación de los estatutos de la Universidad de Castilla-La Mancha.
- Código de conducta de protección de datos personales en la Universidad de Castilla-La Mancha.
- Normativa de utilización de medios electrónicos en la actividad de la administración de la Universidad de Castilla-La Mancha.

8. Organización de la seguridad de la información

La gestión de la seguridad de la información en la Universidad de Castilla-La Mancha estará organizada según la siguiente estructura:

- Responsable de la Información.
- Responsable de los Servicios.
- Responsable del Sistema.
- Responsable de Seguridad de la Información.
- Delegado de Protección de Datos
- Comité de Ciberseguridad.
- Oficina de Ciberseguridad.

- Centro de Operaciones de Ciberseguridad.

Los roles de Responsable de la Información, Responsable de los Servicios, Responsable del Sistema, Responsable de la Seguridad de la Información y Delegado de Protección de Datos serán desempeñados por personas diferentes y actuarán de forma independiente en la realización de las funciones que tienen encomendadas en esta Política de Seguridad. En concreto y de conformidad con el artículo 11 del RD 311/2022, de 3 de mayo, sobre diferenciación de responsabilidades, "la responsabilidad de la seguridad de los sistemas de información estará diferenciada de la responsabilidad sobre la explotación de los sistemas de información concernidos".

8.1. Responsable de la Información

El Responsable de la Información será el Secretario/a General, que tendrá las siguientes funciones y responsabilidades:

- Establecer y elevar para su aprobación por el Comité de Ciberseguridad los requisitos en materia de seguridad aplicables a la Información o niveles de seguridad dentro del marco establecido en el Anexo I del ENS, pudiendo recabar una propuesta al Responsable de Seguridad y teniendo en cuenta la opinión del Responsable del Sistema.
- Dictaminar respecto a los derechos de acceso a la información.
- Aceptar los niveles de riesgo residual que afectan a la información.
- Poner en comunicación del Responsable de Seguridad cualquier variación respecto a la Información, especialmente la incorporación de nueva información. El cual dará traslado de dichos cambios al Comité de Ciberseguridad para su supervisión y validación.

8.2. Responsable de los Servicios

El Responsable de los Servicios será el/la Gerente/a, que tendrá las siguientes funciones y responsabilidades:

- Establecer y elevar para su aprobación por el Comité de Ciberseguridad los requisitos en materia de seguridad aplicables a los Servicios o niveles de seguridad dentro del marco establecido en el Anexo I del ENS, pudiendo recabar una propuesta al Responsable de Seguridad y teniendo en cuenta la opinión del Responsable del Sistema.
- Dictaminar respecto a los derechos de acceso a los servicios.
- Aceptar los niveles de riesgo residual que afectan a los servicios.
- Poner en comunicación del Responsable de Seguridad cualquier variación respecto a los Servicios, especialmente la incorporación de nuevos servicios. El cual dará traslado de dichos cambios al Comité de Ciberseguridad para su supervisión y validación.

8.3. Responsable del Sistema

El Responsable del Sistema será el/la director/a del Área de Tecnología y Comunicaciones, que tendrá las siguientes funciones y responsabilidades:

- Desarrollar, operar y mantener los sistemas de información durante todo su ciclo de vida, elaborando los procedimientos operativos necesarios.
- Definir la topología y la gestión de los sistemas de información estableciendo los criterios de uso y los servicios disponibles en cada uno de ellos.
- Detener el acceso a información o la prestación de un servicio si tiene conocimiento de que estos presentan deficiencias graves de seguridad. Esta decisión deberá ser acordada con el Responsable de la Información, del Servicio y de Seguridad, antes de ser ejecutada.

- Velar por la implantación de las medidas de seguridad que afecten a los servicios e infraestructuras de los que es responsable.
- Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.
- Proporcionar asesoramiento para la determinación de la categoría del Sistema, en colaboración con el Responsable de Seguridad y/o Comité de Ciberseguridad.
- Participar en la elaboración e implantación de los planes de mejora de la seguridad y, llegado el caso, los planes de continuidad.
- Llevar a cabo, en su caso, las funciones del administrador de la seguridad del sistema:

    a) La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad.
    b) La gestión de las autorizaciones concedidas a los usuarios del sistema, en particular los privilegios concedidos, incluyendo la monitorización de la actividad desarrollada en el sistema y su correspondencia con lo autorizado.
    c) Aprobar los cambios en la configuración vigente de los sistemas de información.
    d) Asegurar que los controles de seguridad establecidos se cumplen estrictamente.
    e) Asegurar que son aplicados los procedimientos aprobados para manejar los sistemas de información.
    f) Supervisar las instalaciones de hardware y software, sus actualizaciones y mejoras para asegurar que la seguridad no está comprometida y que en todo momento se ajustan a las autorizaciones pertinentes.
    g) Monitorizar el estado de seguridad proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica.
    h) Informar al Responsable de Seguridad de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.
    i) Colaborar en la investigación y resolución de los incidentes de seguridad, desde su detección hasta su resolución.

8.4. Responsable de Seguridad de la Información

El Responsable de Seguridad de la Información será la persona designada por el Rector para desempeñar las siguientes funciones y responsabilidades:

- Mantener y verificar el nivel de seguridad de la información manejada y de los servicios prestados siguiendo las directrices marcadas por el Comité de Ciberseguridad y de acuerdo a lo establecido en esta Política de Seguridad.
- Promover la formación y concienciación en materia de seguridad de la información siguiendo las directrices marcadas por el Comité de Ciberseguridad.
- Designar responsables de la ejecución del análisis de riesgos, de la Declaración de Aplicabilidad, identificar medidas de seguridad, determinar las configuraciones necesarias, elaborar documentación relativa a la seguridad de los sistemas de información.
- Proporcionar asesoramiento para la determinación de la categoría del Sistema, en colaboración con el Responsable del Sistema y/o Comité de Ciberseguridad.
- Participar en la elaboración e implantación de los planes de mejora de la seguridad y, llegado el caso, en los planes de continuidad, procediendo a su validación.
- Gestionar las revisiones del sistema.
- Gestionar los procesos de certificación del cumplimiento de las obligaciones en materia de seguridad.
- Elevar al Comité de Ciberseguridad la aprobación de cambios y otros requisitos del sistema.

- Aprobar los procedimientos de seguridad que forman parte del conjunto normativo de la seguridad de la información, que no sean competencia del Comité de Ciberseguridad, y poniendo en conocimiento de este Comité las modificaciones que se hayan realizado.

8.5. Delegado de Protección de Datos

El Delegado de Protección de Datos será la persona designada por el Rector para desempeñar las siguientes funciones y responsabilidades:

- Informar y asesorar a la Universidad, y a los usuarios que se ocupen del tratamiento de datos personales, de las obligaciones que les incumben en virtud de la normativa vigente en materia de Protección de Datos.
- Supervisar el cumplimiento de lo dispuesto en la normativa de seguridad y en las políticas de la Universidad en materia de protección de datos, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes.
- Ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos personales y supervisar su aplicación.
- Cooperar con la Agencia Española de Protección de Datos cuando ésta lo requiera, actuando como punto de contacto con ésta para cuestiones relativas al tratamiento de datos personales.

El Delegado de Protección de Datos desempeñará sus funciones prestando atención a los riesgos asociados a las operaciones de tratamiento. Para ello debe ser capaz de:

- Recabar información para determinar las actividades de tratamiento y supervisar su registro en el Registro de Actividades de Tratamiento.
- Analizar y comprobar la conformidad de las actividades de tratamiento.
- Informar, asesorar y emitir recomendaciones al responsable o el encargado del tratamiento.
- Asesorar sobre el principio de la protección de datos por defecto y desde el diseño.
- Asesorar sobre si se es o no necesario realizar las evaluaciones de impacto y sobre la metodología y salvaguardas a aplicar.
- Asesorar al responsable del tratamiento sobre las acciones a priorizar según los riesgos a los que estén sometidos los tratamientos y sobre los que necesiten una mayor dedicación de tiempo y recursos dada su naturaleza y tipología.
- Asesorar al responsable del tratamiento en la realización de auditorías de cumplimiento y sobre las necesidades de formación en materia de protección de datos personales.

8.6. Comité de Ciberseguridad

Se crea el Comité de Ciberseguridad como un órgano colegiado con funciones consultivas y estratégicas para la toma de decisiones en materia de Seguridad de la Información y que estará constituido por:

- **Presidente**: Vicerrector/a competente en materia de seguridad de la información.
- **Secretario**: Secretario/a General.
- **Miembros**:
    a) Responsable de la Información
    b) Responsable de los Servicios.
    c) Responsable del Sistema.
    d) Responsable de Seguridad de la Información.
    e) Delegado de Protección de Datos.
- **Otros miembros no permanentes**:

a) El Comité de Ciberseguridad podrá convocar a sus reuniones a los asesores u otros representantes de la universidad que se consideren oportunos o necesarios para los temas a tratar, con voz, pero sin voto.
b) Así mismo, el Comité podrá solicitar el asesoramiento de especialistas externos a la universidad que se considere necesario por su experiencia y vinculación con los asuntos tratados, con voz, pero sin voto.

Serán funciones propias del Comité:

- Elaboración de la política de seguridad y su revisión periódica, velando por su cumplimiento.
- Elaboración de la normativa de seguridad y su revisión periódica, velando por su cumplimiento.
- Divulgación de la política y normativa de seguridad.
- Aprobación de los procedimientos y directrices en materia de ciberseguridad.
- Aprobación de otras normas, criterios y buenas prácticas en materia de adecuación y certificación de conformidad con el Esquema Nacional de Seguridad (ENS).
- Coordinación de las actuaciones en materia de seguridad de la información para asegurar que estas sean consistentes y estén alineadas con lo establecido en el ENS y la Declaración de aplicabilidad de las medidas de seguridad.
- Supervisión, coordinación y aprobación de las tareas de adecuación y seguimiento del ENS:
    a) Valoración de la información y los servicios.
    b) Categorización del sistema de información.
    c) Análisis de riesgos.
    d) Planes de mejora.
    e) Auditorías.
    f) Certificación de conformidad con el ENS de los servicios prestados por la universidad.
- Aprobación y seguimiento de las iniciativas y objetivos estratégicos en ciberseguridad, velando por la disponibilidad de los recursos necesarios para su desarrollo e implantación.
- Aprobación previa de las propuestas e iniciativas en materia de ciberseguridad que requieran de su aprobación formal por el Consejo de Gobierno.
- Promoción de la formación y la concienciación en materia de ciberseguridad.

8.7. Oficina de Ciberseguridad

Dentro de la estructura de gobernanza de la ciberseguridad se constituye la Oficina de Ciberseguridad, cuyas competencias estarán relacionadas con las siguientes áreas de trabajo: adecuación al ENS, normativa, análisis y gestión de riesgos y mejora continua de la seguridad, así como otras funciones conexas o concordantes. Estará constituida por:

- **Director de la Oficina de Ciberseguridad**, que será el Responsable de Seguridad o la persona designada por el Comité de Ciberseguridad.
- **Secretario de la Oficina de Ciberseguridad**, nombrado por el Comité de Ciberseguridad, a propuesta de los miembros de la Oficina de Ciberseguridad.
- **Administradores de seguridad**, que serán las personas especializadas en seguridad que el Comité de Ciberseguridad determine que son necesarias.

Las funciones de la Oficina de Ciberseguridad serán, entre otras que les puedan ser encomendadas por el Comité de Ciberseguridad:

- Gestión y operativa del proyecto de adecuación, implantación y gestión de la conformidad con el ENS.

- Gestión y operativa del sistema de gestión de la seguridad de la información, promoviendo su mejora continua.
- Gestión y operativa del análisis y gestión de los riesgos y propuesta de aplicación de medidas de seguridad para su minimización.
- Seguimiento de los principales riesgos residuales asumidos por la Universidad y propuesta de posibles actuaciones respecto de ellos.
- Redacción de propuestas relacionadas con la ciberseguridad para su presentación al Comité de Ciberseguridad.
- Elaboración y revisión de la Política de Seguridad de la Información para su validación por el Comité de Seguridad y posterior aprobación por el Consejo de Gobierno.
- Elaboración y revisión de la Normativa sobre la utilización de los sistemas de información y recursos informáticos de la Universidad para su validación por el Comité de Seguridad y posterior aprobación por el Consejo de Gobierno.
- Revisión y validación de los procedimientos de seguridad de la información y demás documentación antes de su aprobación.
- Elaboración de programas de formación y concienciación para formar y sensibilizar al personal en materia de seguridad de la información y protección de datos.
- Elaboración y aprobación de los requisitos de formación y calificación de administradores, operadores y usuarios desde el punto de vista de seguridad de la información.
- Redacción y presentación de propuestas y planes de mejora relacionados con la ciberseguridad al Comité de Ciberseguridad, priorizando las actuaciones y acompañándolas de las estimaciones económicas y presupuestarias correspondientes.
- Promover la realización de las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones de la Universidad en materia de seguridad de la información y protección de datos.
- Aquellas otras funciones que le pueda ser encomendadas por el Comité de Ciberseguridad.

8.8. Centro de Operaciones de Ciberseguridad

Bajo la responsabilidad y dirección de la Oficina de Ciberseguridad de la universidad, o de la persona designada por el Comité de Ciberseguridad, el Centro de Operaciones de Ciberseguridad presta servicios de ciberseguridad, desarrollando la capacidad de vigilancia y detección de amenazas en la operación diaria de los sistemas TIC, a la vez que mejora la capacidad de respuesta del sistema ante cualquier ataque.

El Centro de Operaciones de Ciberseguridad llevará a cabo las siguientes funciones:

- Vigilancia y monitorización de los sistemas y de los dispositivos de defensa.
- Detección de amenazas mediante análisis y correlación de eventos de seguridad y registros de actividad de los sistemas.
- Operaciones de seguridad sobre los dispositivos de defensa.
- Gestión de vulnerabilidades de aplicaciones y servicios mediante el análisis y determinación de las acciones de subsanación y aplicación de actualizaciones.
- Análisis forense digital y de seguridad.
- Mejora de la capacidad de respuesta de los sistemas ante cualquier ataque, pudiendo desempeñar funciones de cibervigilancia que posibilite anticiparse a las ciberamenazas.
- Aquellos otros que se consideren necesarios relacionados con las alertas de seguridad en las redes corporativas y en las conexiones a Internet de los sistemas y con la respuesta a incidentes de seguridad, tales como:
    a) Constituir un Equipo de Respuesta a Incidentes de Seguridad (CERT, por sus siglas en inglés, *Computer Emegency Response Team*), realizando un

seguimiento de la gestión de los incidentes de seguridad y recomendando posibles actuaciones respecto de ellos.

b) Ser un Servicio de Alerta Temprana (SAT) de las alertas de seguridad en las redes corporativas y en las conexiones a Internet de los sistemas.

El Área de Tecnología y Comunicaciones deberá, por un lado, coordinarse con la Oficina de Ciberseguridad en la definición y aplicación de las medidas de seguridad en los sistemas e infraestructuras que estén bajo su responsabilidad; y por el otro, colaborar con el Centro de Operaciones de Ciberseguridad en las tareas de operativa diaria.

Si no se dispusiese de recursos suficientes para disponer de un Centro de Operaciones de Ciberseguridad, el Área de Tecnología y Comunicaciones podrá asumir, en colaboración con la Oficina de Ciberseguridad, en todo o en parte, las funciones propias del mismo.

9. Protección de datos de carácter personal

Sólo se recogerán y tratarán datos personales cuando sean adecuados, pertinentes y no excesivos y estos se utilicen en el ámbito y para las finalidades para los que se hayan obtenido. De igual modo, se adoptarán las medidas de índole técnica y organizativas necesarias para el cumplimiento de la normativa de Protección de Datos.

La Universidad publicará su Política de Privacidad, el Registro de Actividades de Tratamiento y el Código de conducta de protección de datos personales en la Universidad de Castilla-La Mancha en su sitio web, accesible a través de la dirección: www.uclm.es/psi.

10. Gestión de riesgos

La gestión de riesgos es parte esencial del proceso de seguridad y ha de realizase de manera continuada con el objetivo de minimizar los riesgos hasta niveles aceptables.

Todos los sistemas sujetos a esta Política deberán realizar un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. 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 o se detecten vulnerabilidades graves.

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

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

El proceso de gestión de riesgos comprenderá la categorización de los sistemas y el análisis de riesgos. El Comité de Ciberseguridad, para armonizar los análisis de riesgos, establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados y seleccionará las medidas de seguridad a aplicar que deberán ser proporcionales a los riesgos y estar justificadas.

Las fases de este proceso se realizarán según lo dispuesto en los Anexos I y II del Real Decreto 311/2022, de 3 de mayo, y siguiendo las normas, instrucciones, guías CCN-STIC y otras recomendaciones para la aplicación del mismo elaboradas por el Centro Criptológico Nacional.

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

11. Notificación de incidentes

De conformidad con lo dispuesto en el artículo 33 del RD 311/2022, de 3 de mayo, la Universidad notificará al Centro Criptológico Nacional aquellos incidentes que tengan un impacto significativo en la seguridad de los sistemas de información en relación con la categorización del sistema recogida en el Anexo I de dicho cuerpo legal, de acuerdo con la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad.

12. Desarrollo de la Política de Seguridad de la Información

Esta Política de Seguridad de la Información se desarrollará por medio de una normativa y recomendaciones de seguridad que afronte aspectos específicos. Corresponde al Comité de Ciberseguridad su revisión anual, proponiendo, en su caso, las mejoras que sean necesarias.

El conjunto normativo de seguridad de la información se desarrollará en tres niveles por ámbito de aplicación, nivel de detalle técnico y obligatoriedad de cumplimiento, de manera que cada norma de un determinado nivel de desarrollo se fundamente en las normas de nivel superior. Dichos niveles de desarrollo normativo son los siguientes:

- Primer nivel: constituido por la Política de Seguridad de la Información, la Normativa sobre la utilización de los sistemas de información y recursos informáticos de la Universidad y otras directrices generales de seguridad.
- Segundo nivel: constituido por las normas de seguridad derivadas de las anteriores.
- Tercer nivel: constituido por procedimientos, guías e instrucciones técnicas, que determinará las acciones o tareas de seguridad a realizar en el desarrollo de un proceso.

Corresponde al Consejo de Gobierno de la Universidad la aprobación de la Política de Seguridad de la Información y la Normativa sobre la utilización de los sistemas de información y recursos informáticos de la Universidad, siendo el Comité de Ciberseguridad el órgano responsable de la aprobación de los restantes documentos y la de su difusión.

Del mismo modo, la presente Política de Seguridad de la Información complementa la Política de Privacidad en materia de protección de datos personales y al Código de conducta de protección de datos personales en la Universidad de Castilla-La Mancha.

La Política y Normativa de seguridad estará a disposición de todos los miembros de la Universidad que necesiten conocerla, y en particular de aquellos que utilicen, operen o administren los sistemas de información y comunicaciones. Estará disponible en la Intranet de la Universidad, a través de la siguiente dirección: Intranet.uclm.es/psi.

13. Obligaciones del personal

Todo el personal de la Universidad de Castilla-La Mancha tiene la obligación de conocer y cumplir esta Política de Seguridad de la Información y las normas de seguridad que de ella se deriven, siendo responsabilidad del Comité de Ciberseguridad disponer los medios necesarios para que sea conocida por todos los afectados.

Dentro de los planes anuales de formación del personal se incluirán acciones formativas en materia de seguridad de la información y protección de datos personales. Asimismo, se establecerá un programa de concienciación continua para atender a todos los miembros de Universidad, en particular a los de nueva incorporación, teniendo en cuenta siempre las disponibilidades presupuestarias.

Las personas con responsabilidad en el uso, operación o administración de sistemas de información 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.

14. Terceras partes

Cuando la Universidad de Castilla-La Mancha preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipes de esta Política de Seguridad de la Información, se establecerán canales para reporte y coordinación de los respectivos Comités de Ciberseguridad y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando la Universidad de Castilla-La Mancha utilice servicios de terceros o ceda información a terceros, se les hará partícipe de esta Política de Seguridad de la Información y de la Normativa sobre la utilización de los sistemas de información y recursos informáticos de la Universidad que ataña a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en esa 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 de Seguridad de la Información.

Cuando algún aspecto de esta Política de Seguridad de la Información 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.

15. Mejora continua

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

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

16. Aprobación y entrada en vigor

Texto aprobado el día <día> de <mes> de <año> por el Consejo de Gobierno de la Universidad de Castilla-La Mancha.

Esta Política se Seguridad de la Información es efectiva desde el día siguiente de su aprobación.