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 la Información y las 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 calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.

Los sistemas 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 (ENS), 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 los 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 7 del *Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.*

Es por ello que esta política establece un marco organizativo y operacional que garantiza la seguridad de los sistemas, los datos y los servicios prestados a través de medios electrónicos, creando las condiciones de confianza necesarias para que los miembros de la comunidad universitaria y los ciudadanos en general puedan ejercer sus derechos y cumplir sus deberes a través de estos medios.

2. Objeto del documento

El presente documento tiene por objeto definir la política en materia de seguridad de la información de la Universidad de Castilla-La Mancha. Con esta política de seguridad de la información 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 en esta materia.

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 la puesta en producción de los sistemas considerando aspectos de seguridad.
- Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
- Revisar periódicamente si las medidas de seguridad establecidas se están aplicando conforme a la definición de aplicabilidad de las mismas. Esta revisión se realizará como máximo cada dos años mediante auditorías internas o externas.

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 9 del ENS.

La monitorización es especialmente relevante en el supuesto de que se establezcan líneas de defensa de acuerdo con el artículo 8 del ENS. Los mecanismos de detección, análisis y reporte llegarán a los responsables de la Información, de la Seguridad, de los Servicios 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 dar respuesta a los potenciales incidentes de seguridad del siguiente modo:

- Se establecerán mecanismos para responder eficazmente a los incidentes de seguridad.
- Se designará un punto de contacto para las comunicaciones con respecto a incidentes detectados en otras administraciones públicas u otros organismos.
- Se establecerán protocolos para el intercambio de información relacionada con cada 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 desarrollarán planes de continuidad de los sistemas TIC como parte del plan general de continuidad de negocio y actividades de recuperación.

3. Ámbito de aplicación

La presente política de seguridad de la información será de aplicación a los sistemas de información de la Universidad de Castilla-La Mancha que da soporte al ejercicio de los derechos y el cumplimiento de los deberes a través de medios electrónicos por los miembros de la comunidad universitaria y los ciudadanos, y a todos los datos, informaciones y servicios utilizados en medios electrónicos que gestione la Universidad en el ejercicio de sus competencias.

De forma concreta la presente política de seguridad es aplicable sobre los siguientes servicios y sistemas TIC que los conforman:

- **Sistemas de Información:**
  - Gestión Académica
  - Gestión Económica
  - Gestión de Recursos Humanos
  - Gestión de la Investigación
  - Gestión de Inventario
  - Registro General
  - Archivo
  - Biblioteca
  - Campus Virtual
  - Correo electrónico corporativo

- **Servicio de Administración Electrónica:**
  - Sede electrónica
  - Bandeja de firma
  - Registro electrónico
  - Escritorio de tramitación
  - Tablón de anuncios electrónico
  - Notificaciones electrónicas
  - Gestor de expedientes electrónico
  - Archivo electrónico

4. Misión de la Organización

La misión de la Universidad de Castilla-La Mancha es preparar para el ejercicio de las actividades profesionales, crear y transmitir ciencia, técnica y cultura, y comprometerse con el desarrollo económico, teniendo a la excelencia como referente para la docencia, la investigación y la transferencia.

Los valores y principios que la inspiran son:

Valores	Principios	Descripción
Institucionales	Autonomía universitaria	Preservar la autonomía universitaria y garantizar un espacio de convivencia intelectual abierto a todos.
	Suficiencia financiera	Mejorar la captación de recursos y racionalizar la cantidad de servicios prestados sin condicionar la calidad
Académicos	Calidad universitaria	Aplicar criterios de calidad para la aprobación de iniciativas basados en un enfoque de mejora continua.
	Compromiso internacional	Adoptar un enfoque proactivo y transversal en la internacionalización latinoamericana y europea.
Éticos	Transparencia informativa	Impulsar la implantación de instrumentos que garanticen la transparencia de las decisiones adoptadas.
	Responsabilidad social	Considerar las repercusiones sociales de las decisiones adoptadas y cómo afectan a los distintos colectivos.

5. 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 15/1999, de 13 de diciembre, de protección de datos de carácter personal.
- Ley Orgánica 6/2001, de 21 de diciembre, de Universidades.
- Ley 59/2003, de 19 de diciembre, de firma electrónica.
- Ley Orgánica 4/2007, de 12 de abril, por la que se modifica la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades.
- Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.
- 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 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.
- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- 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.
- Decreto 160/2003 de 22 de julio por el que se aprueban los Estatutos de 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.
- Código de conducta de protección de datos personales en la Universidad de Castilla-La Mancha.

6. Organización de la seguridad de la información

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

- Comisión de Tecnología de la Información y las Comunicaciones y de Seguridad Informática, como unidad consultiva dependiente del Consejo de Gobierno.
- Comité de Seguridad de la Información.
- El Responsable de la Información.
- El Responsable de los Servicios.
- El Responsable del Sistema de Información.
- El Responsable de la Seguridad.

6.1. Comisión de Tecnología de la Información y las Comunicaciones y de Seguridad Informática

Entre las funciones de la Comisión de Tecnología de la Información y las Comunicaciones y de Seguridad Informática se encuentran:

- Aprobación previa de la Política de Seguridad antes de ser sometida a la aprobación definitiva por el Consejo de Gobierno.
- Aprobación de la normativa de seguridad.
- Divulgación de la política y normativa de seguridad.
- Aprobación de las iniciativas y de los objetivos estratégicos en seguridad de las TIC.

6.2. El Comité de Seguridad de la Información

Se crea el Comité de Seguridad de la Información, que estará formado por:

- El Secretario General, o vicerrector que ostente las competencias en materia de los sistemas de información, que será su presidente
- Un vicerrector designado por el rector
- El responsable de los Servicios
- El responsable del Sistema
- El responsable de la Seguridad, que actuará como secretario

Serán funciones propias de este Comité:

- Revisión anual de la política de seguridad.
- Desarrollo del procedimiento de designación de roles.
- Designación de roles y responsabilidades.
- Supervisión y aprobación de las tareas de seguimiento del ENS:
    a) Tareas de adecuación
    b) Análisis de riesgos
    c) Auditoría bienal
- Velar por el cumplimiento de la política de seguridad.
- Velar por el cumplimiento de las normativas en materia de seguridad.

- Definición y seguimiento de las iniciativas y los objetivos estratégicos en seguridad de las TIC.
- Fijar las condiciones para satisfacer los requisitos de seguridad de la información.
- Aprobar los procedimientos de seguridad.
- Velar por la disponibilidad de los recursos necesarios para desarrollar las iniciativas y objetivos estratégicos de seguridad necesarios.
- Impulsar la elaboración de directrices en materia de seguridad de la información.
- Promover la formación y concienciación en materia de seguridad de la información.
- Asesorar a la Comisión TIC y de Seguridad Informática en todo lo que solicite e informarle sobre el estado de la seguridad.

6.3. El Responsable de la Información

El Responsable de la Información será el Secretario General de la Universidad o vicerrector competente en materia de sistemas de información, que tendrá las siguientes funciones y responsabilidades:

- Establecimiento de los requisitos de seguridad que garanticen el tratamiento de la información.
- Trabajo en colaboración con el Responsable de Seguridad y el Responsable del Sistema en la valoración de la información en las diferentes dimensiones de seguridad y el mantenimiento de los sistemas catalogados según el Anexo I del ENS.
- Velar por la inclusión de cláusulas sobre seguridad en los contratos con terceras partes y por su cumplimiento.

6.4. El Responsable de los Servicios

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

- Establecimiento de los requisitos de los servicios prestados a través de medios electrónicos en materia de seguridad.
- Trabajo en colaboración con el Responsable de Seguridad y el Responsable del Sistema en la valoración de los servicios en las diferentes dimensiones de seguridad y el mantenimiento de los sistemas catalogados según el Anexo I del ENS.

6.5. El Responsable del Sistema

El Responsable del Sistema será el director del Área de Tecnología y Comunicaciones, que tendrá 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.
- 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.
- Determinar la categoría del sistema según el procedimiento descrito en el Anexo I del ENS y determinar las medidas de seguridad que deben aplicarse según se describe en el Anexo II del ENS.
- Además, puede 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 el Responsable de la Información, el Responsable del Servicio y el Responsable de Seguridad, antes de ser ejecutada.

6.6. El Responsable de Seguridad

El Responsable de Seguridad, que será designado por el Rector, tendrá las siguientes funciones y responsabilidades:

- Mantener la seguridad de la información manejada y de los servicios prestados siguiendo las directrices marcadas por el Comité de Seguridad de la Información y de acuerdo a lo establecido en la Política de Seguridad.
- Promover la formación y concienciación en materia de seguridad siguiendo las directrices marcadas por el Comité de Seguridad de la Información.
- Elaborar las propuestas de modificación y actualización de la política de seguridad de la información.
- Promover para su aprobación y seguimiento en el Comité de Seguridad de la Información las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones en materia de seguridad.
- Desarrollar la política de seguridad de la información mediante la elaboración de la normativa de seguridad.
- Analizar, completar y aprobar toda la documentación relacionada con la seguridad del sistema.
- Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría implementados en el sistema.
- Apoyar y supervisar la investigación de los incidentes de seguridad desde su notificación hasta su resolución.
- Proponer para su aprobación y seguimiento en el Comité de Seguridad de la Información, las líneas de actuación en materia de seguridad de la información.

7. Gestión de la seguridad de la información

La normativa sobre seguridad de la información será de obligado cumplimiento y se desarrollará en tres niveles:

- Primer nivel: política de seguridad de la información.
- Segundo nivel: normativa de seguridad de la información, constituido por el conjunto de normas que desarrollan la política de seguridad y que regulan qué se puede hacer y qué no desde el punto de vista de la seguridad.

- Tercer nivel: de procedimientos técnicos, constituido por el conjunto de procedimientos técnicos que incluyen los detalles de implementación y de tecnología necesarios para realizar una tarea respetando las normas de seguridad.

Estas normas serán elaboradas y aprobadas por los órganos competentes, y se publicarán adecuadamente. Además de los documentos citados, la documentación de seguridad podrá contar con otros documentos como recomendaciones, buenas prácticas, informes, registros, evidencias electrónicas, etc.

8. Protección de datos de carácter personal

Todos los ficheros y tratamientos de datos de carácter personal se ajustarán a los niveles de seguridad requeridos por la normativa aplicable según la naturaleza y la finalidad de los datos. En el Documento de Seguridad de la Universidad de Castilla-La Mancha se incluyen los ficheros y tratamientos de datos de carácter personal, así como las medidas de seguridad que le son de aplicación y los responsables internos de los mismos.

9. 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
- cuando se reporten vulnerabilidades graves

Para la armonización de los análisis de riesgos, el Comité de Seguridad de la Información establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados.

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

10. Desarrollo de la Política de Seguridad de la Información

Esta Política de Seguridad de la Información se desarrollará por medio de normativa de seguridad que afronte aspectos específicos. La 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.

La normativa de seguridad estará disponible en la intranet corporativa, a través de la dirección https://intranet.uclm.es/psi/.

11. Obligaciones del personal

Todos los miembros de la Universidad de Castilla-La Mancha tienen 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 Seguridad de la Información disponer los medios necesarios para que sea conocida por todos los afectados.

Todos los trabajadores recibirán una sesión de concienciación en materia de seguridad TIC cada dos años. 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 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.

12. 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 Seguridad TIC 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 y de la Normativa de Seguridad que ataña a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en esta 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.

13. Aprobación y entrada en vigor

Texto aprobado el día 13 de abril de 2015 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.