POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE LA UNIVERSITAT POLITÈCNICA DE VALÈNCIA

Aprobada por el Consejo de Gobierno de 16 de abril de 2019 y modificada por el Consejo de Gobierno de 10 de noviembre de 2022

1. INTRODUCCIÓN

La Universitat Politècnica de València depende de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar sus objetivos. Estos sistemas deben ser administrados con diligencia, garantizando su resiliencia 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.

La seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema de información, 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.

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 se deben aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad (ENS), regulado por el Real Decreto 3/2010 de 8 de enero, 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.

Todos los miembros de la comunidad universitaria, el personal y los responsables de las estructuras organizativas y de los servicios universitarios de la Universitat Politècnica de València deben interiorizar e incorporar a su práctica diaria el valor de la seguridad. La Universitat debe estar preparada para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo al artículo 7 del Esquema Nacional de Seguridad.

Editor: Secretaria General / UPV · D.L.: V-5092-2006 · ISSN: 1887-2298 · www.upv.es/secgen

I[1]

Mediante acuerdo del Consejo de Gobierno de 16 de abril de 2019 fue aprobada la Política de seguridad de la información de la Universitat Politècnica de València.

Por otro lado, la Guía de Seguridad de las TIC, CCN-STIC 881, que recoge la Guía de adecuación al Esquema Nacional de Seguridad (ENS) para la Universidad, se publicó en mayo de 2022, junto con su anexo en el que se describe cómo debería ser la redacción de la Política de Seguridad de las Universidades. Entre otras cuestiones, en el epígrafe 3.1 de la Guía se recoge la composición del Comité de Seguridad de la Información, señalando que entre los miembros permanente del mismo deberá figurar el Responsable de Seguridad de la Información, indicando que será designado por el Rector de la Universidad o el equipo de dirección.

Así pues, dado que la Política de Seguridad de la Información de la Universitat Politècnica de València recoge en su apartado 6.2 el procedimiento de designación del Responsable de Seguridad de la Información, no siendo coincidente con lo propuesto en la Guía de Seguridad de las TIC antes señalada, resulta necesario realizar la adaptación de este apartado de la Política de Seguridad de la Información de la Universitat Politècnica de València.

Por todo ello, el Consejo de Gobierno, a propuesta de la Comisión Permanente, propone la aprobación de la siguiente propuesta de modificación de la Política de Seguridad de la Información de la Universitat Politècnica de València.

2. ÁMBITO DE APLICACIÓN

Esta política se aplica a todos los sistemas TIC de la Universitat Politècnica de València y a todos los miembros de la comunidad universitaria, sin excepciones.

3. MISIÓN

La Universitat Politècnica de València forma a personas para potenciar sus competencias; investiga y genera conocimiento, con calidad, rigor y ética, en los ámbitos de la ciencia, la tecnología, el arte y la empresa, con el objetivo de impulsar el desarrollo integral de la sociedad y contribuir a su progreso tecnológico, económico y cultural.

En el desempeño de su misión, la seguridad cumple una función esencial para afianzar los objetivos de la Universitat mediante el uso de sus sistemas de información, con el fin último de garantizar los derechos fundamentales de sus usuarios.

4. MARCO NORMATIVO

Los Estatutos de la Universitat Politècnica de València, junto con su normativa de desarrollo, constituyen el marco en el que encuadrar esta política.

[1] Texto introducido por el Acuerdo del Consejo de Gobierno de 10 de noviembre de 2022.

Asimismo, se tendrá en cuenta la legislación vigente en cuanto a protección de datos, propiedad intelectual y uso de herramientas telemáticas. Y en concreto el Reglamento de la Unión Europea 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, la Ley Orgánica 3/2018 de Protección de Datos Personales y Garantía de los Derechos Digitales, la Ley 39/2015 de Procedimiento Administrativo Común de las Administraciones Públicas, Ley 40/2018, de Régimen Jurídico del Sector Público y el Real Decreto 3/2010, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración Electrónica.

5. DATOS DE CARÁCTER PERSONAL

La Universitat Politècnica de València trata datos de carácter personal, aplicando en su tratamiento las medidas de seguridad adecuadas teniendo en cuenta el estado de la técnica, costes de aplicación, y la naturaleza, alcance, contexto y fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas.

Así mismo se aplicarán las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo detectado, con la finalidad de asegurar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento

6. ORGANIZACIÓN DE LA SEGURIDAD

6.1. ROLES: FUNCIONES Y RESPONSABILIDADES

6.1.1. El Responsable de Seguridad de la Información

Tendrá entre sus funciones:

a. 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 la Política de Seguridad de la Organización.
b. Promover la formación y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad.
c. Participar en los análisis de riesgo, ayudando a determinar la categoría del Sistema y estableciendo la declaración de aplicabilidad y las medidas de seguridad adicionales.
d. 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.

6.1.2. El Comité de Seguridad TIC

Actuará como Responsable de la Información en la Universitat Politècnica de València, siendo el responsable de establecer los requisitos de la información en materia de seguridad.

El Comité de Seguridad TIC tendrá el rol de Responsable del Servicio en la Universitat, teniendo la potestad de determinar los niveles de seguridad de los servicios, atendiendo a los requisitos

de seguridad de la información y añadiendo los requisitos de disponibilidad, accesibilidad, interoperabilidad, etc. necesarios.

El Comité de Seguridad de la Información no es un comité técnico, pero recabará regularmente del personal técnico propio o externo, la información pertinente para tomar decisiones. El Comité de Seguridad de la Información se asesorará de los temas sobre los que tenga que decidir o emitir una opinión. Este asesoramiento se determinará en cada caso, pudiendo materializarse de diferentes formas y maneras mediante:

a. Grupos de trabajo especializados internos, externos o mixtos.
b. Asesoría externa.
c. Asistencia a cursos u otro tipo de entornos formativos o de intercambio de experiencias

6.1.3. Jefaturas de servicio del ámbito competente en materia TIC

Las personas que desempeñan las jefaturas de servicio del ámbito competente en materia TIC tendrán la función de Responsables de Sistemas.

Tendrán como responsabilidades:

a. Desarrollar, operar y mantener el Sistema de Información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.
b. Definir la topología y sistema de gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo.
c. Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.
d. Actuarán como Administradores de la Seguridad de Sistemas las personas con el cargo de Jefe de Servicios del ámbito competente en materia TIC. Entre sus funciones se encuentran:
    d.1. La implementación, gestión y mantenimiento de las medidas de seguridad aplicables al Sistema de Información.
    d.2. 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.
    d.3. 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.
    d.4. La aplicación de los Procedimientos Operativos de Seguridad.
    d.5. Aprobar los cambios en la configuración vigente del Sistema de Información.
    d.6. Asegurar que los controles de seguridad establecidos son cumplidos estrictamente.
    d.7. Asegurar que son aplicados los procedimientos aprobados para manejar el sistema de información.
    d.8. 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.

Editor: Secretaria General / UPV · D.L.: V-5092-2006 · ISSN: 1887-2298 · www.upv.es/secgen

d.9. Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica implementados en el sistema.
d.10. Informar a los Responsables de la Seguridad y del Sistema de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.
d.11. Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución.

6.2. PROCEDIMIENTOS DE DESIGNACIÓN

El nombramiento del Responsable de Seguridad de la Información y la designación de los Responsables identificados en esta Política, se realizarán por el rector de la Universitat Politècnica de València. El nombramiento se revisará, al menos, cada cuatro años o cuando el puesto quede vacante.

6.3. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Será misión del Comité de Seguridad TIC la revisión anual de esta Política de Seguridad de la Información y la propuesta de revisión o mantenimiento de la misma.

La Política será aprobada por el Consejo de Gobierno y difundida para que la conozcan todas las partes afectadas.

7. PREVENCIÓN

La Universitat Politècnica de València debe evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean afectados por incidentes de seguridad. Para ello se 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 y documentados.

Para garantizar el cumplimiento de esta Política, la Universitat debe:

a. Autorizar los sistemas antes de entrar en operación, aplicando los principios de seguridad desde el diseño y por defecto.
b. Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
c. Solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

8. DETECCIÓN

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, los servicios deben monitorizar la operación de

manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia según lo establecido en el artículo 9 del Esquema Nacional de Seguridad.

La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el artículo 8 del Esquema Nacional de Seguridad. 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.

9. RESPUESTA

La Universitat Politècnica de València debe:

a. Establecer mecanismos para responder eficazmente a los incidentes de seguridad.
b. Designar punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos.
c. 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)

10. RECUPERACIÓN

Para garantizar la disponibilidad de los servicios críticos, la organización debe desarrollar planes de continuidad de los sistemas TIC como parte de su plan general de continuidad de negocio y actividades de recuperación.

11. 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.

Este análisis se llevará a cabo en los siguientes supuestos:

a. De forma regular, al menos una vez cada dos años.
b. En el caso de que se cambie la información manejada.
c. En el caso de que cambien los servicios prestados.
d. Siempre que ocurra un incidente grave de seguridad.
e. En todo caso cuando se reporten vulnerabilidades graves.
f. En cualquier momento que sea necesario conforme a lo establecido en la normativa de protección de datos personales.

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.

12. DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Esta Política 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 Universitat Politècnica de València que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

La normativa de seguridad estará disponible en la Intranet de la Universitat Politècnica de València.

13. OBLIGACIONES DEL PERSONAL

Todos los miembros de la Universitat Politècnica de València 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 disponer los medios necesarios para que la información llegue a los afectados.

Todos los miembros de la Universitat Politècnica de València atenderán a sesiones de concienciación en materia de seguridad TIC. Se establecerá un programa de concienciación continua para atender a todos los miembros de la misma, en particular a los de nueva incorporación.

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.

14. TERCERAS PARTES

Cuando la Universitat Politècnica de València preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipes a estos 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 Universitat Politècnica de València utilice servicios de terceros o ceda información a terceros, se les hará partícipes a estos 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

Editor: Secretaria General / UPV · D.L.: V-5092-2006 · ISSN: 1887-2298 · www.upv.es/secgen

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. ENTRADA EN VIGOR

a. Esta Política de Seguridad de la Información es efectiva desde la aprobación por el Consejo de Gobierno y hasta que sea reemplazada por una nueva Política.
b. Asimismo, esta Política de Seguridad de la Información será publicada en el Butlletí Oficial de la Universitat Politècnica de València (BOUPV).

Editor: Secretaria General / UPV · D.L.: V-5092-2006 · ISSN: 1887-2298 · www.upv.es/secgen