BOUPV
Butlletí Oficial de la Universitat Politècnica de València



# POLÍTICA DE SEGURIDAD DE LA UNIVERSITAT POLITÈCNICA DE VALÈNCIA

*Aprobada por Consejo de Gobierno de 6 de junio de 2024*[1]



[1] Esta política de seguridad tiene su origen en la política de seguridad aprobada por Consejo de Gobierno de 16 de abril de 2019 y modificada por Consejo de Gobierno de 10 de noviembre de 2022.

1. Aprobación y entrada en vigor

Texto aprobado el 6 de junio de 2024 por acuerdo de Consejo de Gobierno de la Universitat Politècnica de València.

Esta "Política de Seguridad de la Información", en adelante Política, será efectiva desde su fecha de aprobación y hasta que sea reemplazada por una nueva Política.

2. Introducción

La Universitat Politècnica de València, depende de los sistemas TIC (Tecnologías de la Información y las Telecomunicaciones) 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 seguridad de la información tratada o los servicios prestados y estando siempre protegidos contra las amenazas o los incidentes con potencial para incidir en la confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad de la información tratada y los servicios prestados.

Para hacer frente a 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 departamentos 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 los servicios, monitorizar y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los ciberincidentes para garantizar la continuidad de los servicios prestados.

De este modo, todas las unidades administrativas de la universidad tienen presente que la seguridad TIC es un proceso 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, basados en la gestión de riesgos, 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.

Por tanto, para la Universitat Politècnica de València, el objetivo de la Seguridad de la Información es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, implantando líneas de defensa y supervisando la actividad diaria para detectar cualquier incidente y reaccionando con presteza a los incidentes para recuperar los servicios lo antes posible, según lo establecido en el artículo 8 del ENS, con la aplicación de las medidas que se relacionan a continuación.

2.1 Prevención

Para que la información y/o los servicios no se vean perjudicados por incidentes de seguridad, la Universitat Politècnica de València implementa las medidas de seguridad establecidas por el ENS, así como cualquier otro control adicional, que haya identificado como necesario, a través de una evaluación de amenazas y riesgos. Estos controles, los roles y responsabilidades de seguridad de todo el personal, están claramente definidos y documentados.

Para garantizar el cumplimiento de la política, la Universitat Politècnica de València:

- Autoriza los sistemas antes de entrar en operación.
- Evalúa regularmente la seguridad, incluyendo el análisis de los cambios de configuración realizados de forma rutinaria.
- Solicita la revisión periódica por parte de terceros, con el fin de obtener una evaluación independiente.

2.2 Detección

La Universitat Politècnica de València, establece controles de operación de sus sistemas de información con el objetivo de detectar anomalías en la prestación de los servicios y actuar en consecuencia según lo dispuesto en el artículo 10 del ENS (vigilancia continua y reevaluación periódica). Cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales (conforme a lo indicado en el artículo 9 del ENS, Existencia de líneas de defensa), se establecerán los mecanismos de detección, análisis y reporte necesarios para que lleguen a los responsables regularmente.

2.3 Respuesta

La Universitat Politècnica de València, establecerá las siguientes medidas:

- Mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar un punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en 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, la Universitat Politècnica de València, dispone de los medios y técnicas necesarias que permiten garantizar la recuperación de los servicios más críticos.

3. Misión

La misión de la Universitat Politècnica de València es la formación integral de los estudiantes a través de la creación, desarrollo, transmisión y crítica de la ciencia, de la técnica del arte y de la cultura, desde el respeto a los principios éticos, con una decidida orientación a la consecución de un empleo acorde con su nivel de estudios.

La contribución al desarrollo cultural, social y económico de la sociedad valenciana y española mediante el apoyo científico, técnico y artístico.

El desarrollo de un modelo de institución caracterizada por los valores de excelencia, internacionalización, solidaridad y eficacia; una institución abierta que incentiva la participación de instituciones, empresas y profesionales en todos los aspectos de la vida universitaria.

Para lograr esta misión, la Universitat Politècnica de València pone a disposición de la ciudadanía la realización de trámites online y nuevas vías de participación que garanticen el desarrollo y la eficacia de sus funciones y cometidos.

Al potenciar el uso de estas tecnologías se persigue fomentar la relación electrónica todos los actores (docentes, estudiantes, investigadores, personal de administración y servicios, y otros) con la universidad.

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 de manera coherente y eficaz la implantación del proceso de seguridad.
- Responsabilidad determinada: En los sistemas TIC se identificará 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.

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

- 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.
- Seguridad por defecto: Los sistemas deben diseñarse y configurarse de forma que garanticen un grado suficiente de seguridad por defecto. Se aplicarán los requisitos mínimos de autorización y control de acceso, protección de las instalaciones, adquisición de productos de seguridad y contratación de servicios de seguridad, Protección de la información, Prevención ante otros sistemas de información interconectados, Registro de la actividad y detección de código dañino, Incidentes de seguridad y Mínimo privilegio.

5. Objetivos de la Seguridad de la Información

La Universitat Politècnica de València, 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 su 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 sus procesos de negocio, de acuerdo con las necesidades de nivel de servicio de sus usuarios.
- Protección de 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. Alcance

Esta Política se aplicará a los sistemas de información de la Universitat Politècnica de València, relacionados con el ejercicio de sus competencias y a todos los usuarios con acceso autorizado a los mismos, sean o no empleados públicos y con independencia de la naturaleza de su relación jurídica con la universidad. Todos ellos tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y su Normativa de Seguridad derivada, siendo responsabilidad del Comité de Seguridad de la Información disponer los medios necesarios para que la información llegue al personal afectado.

## 7. Marco normativo

El marco normativo en que se desarrollan las actividades de la Universitat Politècnica de València y, en particular, la prestación de sus servicios electrónicos está integrado por las normas que se referencian en el anexo: “Anexo Legal - Política de Seguridad de la Información de la Universitat Politècnica de València”.

8. Organización de la Seguridad de la Información

8.1 Criterios utilizados para la organización de la Seguridad de la Información

La Universitat Politècnica de València, teniendo en cuenta lo establecido en el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS), para organizar la seguridad de la información emprenderá las siguientes acciones:

i. Designará roles de seguridad: Responsables de los Servicios, Responsables de la Información, Responsable de Seguridad, Responsable del Sistema y Delegado de Protección de Datos.
ii. Constituirá un órgano consultivo y estratégico para la toma de decisiones en materia de Seguridad de la Información. Este órgano se constituirá como un órgano colegiado y se denominará Comité de Seguridad de la Información. Será presidido por una persona física que será la que asumirá la responsabilidad formal de sus actos.

8.2 Roles y Órganos de la Seguridad de la Información

En la Universitat Politècnica de València, en el marco del ENS, los roles y órganos de la Seguridad de la Información, serán los siguientes:

- Responsable de la Información y los Servicios.
- Responsable de Seguridad de la Información
- Responsable del Sistema
- Comité de Seguridad de la Información

8.2.1 Procedimientos de designación

- La creación del Comité de Seguridad de la Información, el nombramiento de sus integrantes y la designación de los Responsables identificados en esta Política, se realizará por el rector de la Universitat Politècnica de València
- El nombramiento se revisará cada 4 años o cuando el puesto quede vacante.

Estará formado por los siguientes miembros:

Miembros permanentes:

Composición:

- Presidente/a: El Vicerrector/a de Planificación, Oferta Académica y Transformación Digital.
- Vicepresidente/a, que sustituirá al presidente/a en caso de vacante, ausencia o enfermedad: el Director/a de Área de Ciberseguridad.
- Secretario/a: Un Técnico/a del Área de Sistemas de Información y las Comunicaciones designado por el Vicerrector/a de Planificación, Oferta Académica y Transformación Digital.

Vocales:

- El Secretario/a General.
- El Gerente/a.
- Dos técnicos/as del Área de Sistemas de Información y las Comunicaciones designados por el Vicerrector/a de Planificación, Oferta Académica y Transformación Digital.
- Tres personas designadas por el rectorado de entre los Órganos de Gobierno, los Servicios Universitarios, las Escuelas o Facultades y los Departamento.

Miembros no permanentes:

Vocales:

- Jefaturas de servicios vinculados con los asuntos a tratar
- El Delegado/a de Protección de Datos de la Universitat.
- Especialistas externos, de los sectores público, privado y/o académico, cuya presencia, por razón de su experiencia o vinculación con los asuntos tratados, sea necesaria o aconsejable.

Las Jefaturas de los Servicios serán convocados por la presidencia en función de los asuntos a tratar.

El Delegado de Protección de Datos participará con voz, pero sin voto en las reuniones del Comité de seguridad de la información cuando en el mismo vayan a abordarse cuestiones relacionadas con el tratamiento de datos de carácter personal, así como siempre que se requiera su participación. En todo caso, si un asunto se sometiese a votación, se hará constar siempre en acta la opinión del Delegado de Protección de Datos.

El Secretario del Comité realizará las convocatorias y levantará actas de las reuniones del Comité de Seguridad de la Información. A las sesiones del Comité de Seguridad de la Información podrán asistir en calidad de asesores las personas que en cada caso estime pertinentes su Presidente.

8.3 Responsabilidades de los roles asociados al Esquema Nacional de Seguridad

8.3.1 Responsable de la Información y los Servicios

Serán funciones de los Responsables de la Información y de los Servicios:

- Establecer los requisitos de seguridad aplicables a la Información (niveles de seguridad de la Información) y a los Servicios (niveles de seguridad de los servicios) en materia de seguridad, 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 y los servicios.
- Aceptar los niveles de riesgo residual que afectan a la información y los servicios.
- Poner en comunicación del Responsable de Seguridad cualquier variación respecto a la Información y los Servicios, especialmente la incorporación de nuevos Servicios o Información.

8.3.2 Responsable de Seguridad de la Información

Serán funciones del Responsable de Seguridad de la Información:

- Mantener y verificar el nivel adecuado de seguridad de la Información manejada y de los Servicios electrónicos prestados por los sistemas de información.
- Promover la formación y concienciación en materia de seguridad de la información.
- Designar responsables de la ejecución del análisis de riesgos, de la Declaración de Aplicabilidad, identificar medidas de seguridad, determinar configuraciones necesarias, elaborar documentación del sistema.
- Proporcionar asesoramiento para la determinación de la Categoría del Sistema, en colaboración con el Responsable del Sistema y/o Comité de Seguridad de la Información.
- 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 externas o internas del sistema.
- Gestionar los procesos de certificación.
- Elevar al Comité de Seguridad la aprobación de cambios y otros requisitos del sistema.
- Aprobar los procedimientos de seguridad que forman parte del Mapa Normativo (y no son competencia del Comité) y poner en conocimiento al Comité de las modificaciones que se hayan realizado a lo largo del periodo en curso.

8.3.3 Responsable del Sistema

Serán funciones del Responsable del Sistema:

- Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida, elaborando los procedimientos operativos necesarios.
- Definir la topología y la gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Detener el acceso a información o prestación de servicio si tiene el conocimiento de que estos presentan deficiencias graves de seguridad.
- 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 Seguridad de la Información.
- Participar en la elaboración e implantación de los planes de mejora de la seguridad y llegado el caso en los planes de continuidad.

- Llevar a cabo, en su caso, las funciones del administrador de la seguridad del sistema:
    - La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad.
    - 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.
    - Aprobar 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.
    - Monitorizar el estado de seguridad proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica.
    - Informar al Responsable de Seguridad 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.

Cuando la complejidad del sistema lo justifique, el Responsable del Sistema podrá designar los responsables de sistema delegados que considere necesarios, que tendrán dependencia funcional directa de aquél y serán responsables en su ámbito de todas aquellas acciones que les delegue el mismo. De igual modo, también podrá delegar en otro/s funciones concretas de las responsabilidades que se le atribuyen.

8.3.4 Delegado de Protección de Datos

Serán funciones del Delegado de Protección de Datos:

- Informar y asesorar a la Universitat Politècnica de València, y a los usuarios que se ocupen del tratamiento, 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 normativa de seguridad y de las políticas internas de la Universitat Politècnica de València, 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 y supervisará 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.
- Actuar como punto de contacto (ventanilla única) con los interesados en lo relativo al tratamiento de sus datos personales y al ejercicio de sus derechos.

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.
- Analizar y comprobar la conformidad de las actividades de tratamiento.
- Informar, asesorar y emitir recomendaciones al responsable o el encargado del tratamiento.
- Recabar información para supervisar el registro de las operaciones de tratamiento.
- Asesorar en el principio de la protección de datos por diseño y por defecto.
- Asesorar sobre si se lleva a cabo o no las evaluaciones de impacto, metodología, salvaguardas a aplicar, etc. o Priorizar actividades en base a los riesgos.
- Asesorar al Responsable de Tratamiento sobre áreas a cometer a auditorías, actividades de formación a realizar y operaciones de tratamiento a dedicar más tiempo y recursos.

8.3.5 Comité de Seguridad de la Información

Serán funciones del Comité de Seguridad de la Información:

a) Estar permanentemente informado de la normativa que regula la Certificación de Conformidad con el ENS, incluyendo sus normas de acreditación, certificación, guías, manuales, procedimientos e instrucciones técnicas.
b) Estar permanentemente informado de la relación de Entidades de
c) Certificación acreditadas y organizaciones, públicas y privadas, certificadas.
d) Estar permanentemente informado de la relación de esquemas de certificación de la seguridad con los que la Administración Pública tiene establecidos arreglos o acuerdos de reconocimiento mutuo de certificados.
e) Proponer directrices y recomendaciones, que serán recogidas en las correspondientes actas de las reuniones del Comité, a las que su presidente, deberá dar cumplida respuesta.
f) Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información, para asegurar que estos sean consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades.
g) Atender las inquietudes, en materia de Seguridad de la Información, de la Administración y de las diferentes áreas, informando regularmente del estado de la seguridad de la información a la Dirección.

h) Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables y/o entre diferentes Departamentos, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.
i) Asesorar en materia de seguridad de la información, siempre y cuando le sea requerido.
j) Revisar la Política de Seguridad de la Información previa aprobación por el Órgano Superior.
k) Aprobar la Normativa de Uso de Medios electrónicos para todo el personal.
l) Aprobar el Mapa de Normativa con la lista de Normativa y Procedimientos de seguridad para la implantación del ENS.
m) Actuará como Responsable de la Información y de los Servicios.

Periodicidad de las reuniones y adopción de acuerdos:

- Durante el desarrollo del Proyecto de Adecuación al ENS, para evaluar el desarrollo del mismo y posibilitar su adecuado seguimiento, el Comité de Seguridad de la Información se reunirá, al menos, una vez al trimestre.
- Una vez alcanzada la Certificación de Conformidad con el ENS de los servicios prestados por la universidad, el Comité de Seguridad de la Información se reunirá, al menos, dos veces al año con carácter semestral, sin perjuicio de que, en atención a las necesidades derivadas del cumplimiento de sus fines y atribuciones, requiera de una mayor frecuencia en las reuniones.
- En cualquier caso, las reuniones se convocarán por su Presidencia, a través del Secretario, a su iniciativa o por mayoría de sus miembros permanentes.
- Las decisiones se adoptarán por consenso de los miembros permanentes.

9. Datos personales

La Universitat Politècnica de València, solo recogerá y tratará datos personales cuando sean adecuados, pertinentes y no excesivos y éstos se encuentren en relación con el ámbito y las finalidades para los que se hayan obtenido. De igual modo, adoptará las medidas de índole técnica y organizativas necesarias para el cumplimiento de la normativa de Protección de Datos.

La Universitat Politècnica de València, publicará en la Sede Electrónica su Política de Privacidad y el Registro de Actividades de Tratamiento.

10. Obligaciones del personal

Todo el personal de la Universitat Politècnica de València, comprendido dentro del ámbito del ENS, atenderá a una o varias sesiones de concienciación en materia de seguridad y protección de datos, al menos una vez al año. Se establecerá un programa de concienciación continua para atender a todo el personal, en particular al de nueva incorporación.

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.

11. Gestión de riesgos

Todos los sistemas afectados por la presente Política de Seguridad de la Información están sujetos a un análisis de riesgos con el objetivo de evaluar las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá:

- Al menos una vez al año.
- Cuando cambien la información y/o los servicios manejados de manera significativa.
- 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 carencias y debilidades y ponerlas en conocimiento del Comité de Seguridad de la Información.

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.

El proceso de gestión de riesgos comprenderá las siguientes fases:

- Categorización de los sistemas.
- Análisis de riesgos.
- El Comité de Seguridad de la Información procederá a la selección de medidas de seguridad a aplicar que deberán de 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 8 de enero, y siguiendo las normas, instrucciones, Guías CCN-STIC y recomendaciones para la aplicación de este 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.

11.1 Riesgos que se derivan del tratamiento de datos personales

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, como la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos, susceptibles en particular de ocasionar daños y perjuicios físicos, materiales o inmateriales.

Se publicará el registro de actividades de su tratamiento y se realizará la gestión de riesgos a través de Análisis de Riesgos y EPID, en el caso que fuese necesario.

12. Notificación de incidentes

De conformidad con lo dispuesto en el artículo 33 del RD 311/2022, de 3 de mayo, la Universitat Politècnica de València, notificará al Centro Criptológico Nacional aquellos incidentes que tengan un impacto significativo en la seguridad de la información manejada y de los servicios prestados en relación con la categorización de sistemas recogida en el Anexo I de dicho cuerpo legal.

13. Desarrollo de la Política de Seguridad de la Información

La presente Política de Seguridad de la Información será complementada por medio de diversa normativa y recomendaciones de seguridad (normativas y procedimientos de seguridad, procedimientos técnicos de seguridad, informes, registros y evidencias electrónicas). Corresponde al Comité de Seguridad de la Información su revisión anual y/o mantenimiento, proponiendo, en caso de que sea necesario mejoras a la misma.

El cuerpo normativo sobre 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:

1. Primer nivel normativo: políticas de seguridad.
2. Segundo nivel normativo: constituido por las normativas de seguridad.
3. Tercer nivel normativo: constituido por procedimientos, guías e instrucciones técnicas. Son documentos que, cumpliendo con lo expuesto en la Política de Seguridad de la Información, determinan las acciones o tareas a realizar en el desempeño de un proceso.

Corresponde al Consejo de Gobierno de la Universitat Politècnica de València la aprobación de la Política de Seguridad de la Información y la Normativa de Seguridad de la Universidad, siendo el Comité de Seguridad de la Información el órgano responsable de la aprobación de los restantes documentos, siendo también responsable de su difusión para que la conozcan las partes afectadas.

Del mismo modo, la presente Política de Seguridad de la Información complementa la Política de Privacidad de la Universitat Politècnica de València, en materia de protección de datos.

La normativa de seguridad y, muy especialmente, la Política de seguridad de la Información será conocida y estará a disposición de todos los miembros de la universidad, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones. Estará disponible para su consulta en la Intranet, en soporte papel, esta documentación será custodiada por el Área de Sistemas de Información y Comunicaciones.

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

14. Terceras partes

Cuando la Universitat Politècnica de València, preste servicios a otros organismos o maneje información de otros organismos, se les hará participe de esta Política de Seguridad de la Información. Se establecerán canales para el reporte y la coordinación de los respectivos Comités de Seguridad de la Información 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 participe 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 de Seguridad.

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:

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

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