POLÍTICA DE SEGURETAT DE LA INFORMACIÓ DE LA UNIVERSITAT POLITÈCNICA DE VALÈNCIA

Aprovada pel Consell de Govern del 16 d'abril del 2019

1. INTRODUCCIÓ

La Universitat Politècnica de València depèn dels sistemes TIC (tecnologies de la informació i les comunicacions) per a aconseguir els seus objectius. Aquests sistemes han de ser administrats amb diligència, cal garantir-ne la resiliència prenent les mesures adequades per a protegir-los davant de danys accidentals o deliberats que puguen afectar la disponibilitat, la integritat o la confidencialitat de la informació tractada o els serveis prestats.

L'objectiu de la seguretat de la informació és garantir la qualitat de la informació i la prestació continuada dels serveis, actuant preventivament, supervisant l'activitat diària i reaccionant amb prestesa als incidents.

La seguretat TIC és una part integral de cada etapa del cicle de vida del sistema d'informació, des de la seua concepció fins a la seua retirada de servei, passant per les decisions de desenvolupament o adquisició i les activitats d'explotació. Els requisits de seguretat i les necessitats de finançament han de ser identificats i inclosos en la planificació, en la sol·licitud d'ofertes, i en plecs de licitació per a projectes de TIC.

Els sistemes TIC han d'estar protegits contra amenaces de ràpida evolució amb potencial per a incidir en la confidencialitat, la integritat, la disponibilitat, l'ús previst i el valor de la informació i els serveis. Per a defensar-se d'aquestes amenaces, es requereix una estratègia que s'adapte als canvis en les condicions de l'entorn per a garantir la prestació contínua dels serveis. Això implica que s'han d'aplicar les mesures mínimes de seguretat exigides per l'Esquema Nacional de Seguretat (ENS), regulat pel Reial decret 3/2010, de 8 de gener, i també dur a terme un seguiment continu dels nivells de prestació de serveis, seguir i analitzar les

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

Aprobada por el Consejo de Gobierno de 16 de abril de 2019

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

vulnerabilitats reportades, i preparar una resposta efectiva als incidents per a garantir la continuïtat dels serveis prestats.

Tots els membres de la comunitat universitària, el personal i els responsables de les estructures organitzatives i dels serveis universitaris de la Universitat Politècnica de València han d'interioritzar i incorporar a la seua pràctica diària el valor de la seguretat. La Universitat ha d'estar preparada per a prevenir, detectar, reaccionar i recuperar-se d'incidents, d'acord amb l'article 7 de l'Esquema Nacional de Seguretat.

2. ÀMBIT D'APLICACIÓ

Aquesta política s'aplica a tots els sistemes TIC de la Universitat Politècnica de València i a tots els membres de la comunitat universitària, sense excepcions.

3. MISSIÓ

La Universitat Politècnica de València forma persones per a potenciar les seues competències; investiga i genera coneixement, amb qualitat, rigor i ètica, en els àmbits de la ciència, la tecnologia, l'art i l'empresa, amb l'objectiu d'impulsar el desenvolupament integral de la societat i contribuir al seu progrés tecnològic, econòmic i cultural.

En l'acompliment d'aquesta missió, la seguretat compleix una funció essencial per a afermar els objectius de la Universitat mitjançant l'ús dels seus sistemes d'informació, amb la finalitat última de garantir els drets fonamentals dels seus usuaris.

4. MARC NORMATIU

Els Estatuts de la Universitat Politècnica de València, juntament amb la normativa que els desenvolupen, constitueixen el marc en el qual enquadrar aquesta política.

Així mateix, es tindrà en compte la legislació vigent quant a protecció de dades, propietat intel·lectual i

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.

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.

Asimismo se tendrá en cuenta la legislación vigente en cuanto a protección de datos, propiedad

ús d'eines telemàtiques. I, en concret, el Reglament de la Unió Europea 2016/679, relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes dades, la Llei orgànica 3/2018 de protecció de dades personals i garantia dels drets digitals, la Llei 39/2015 de procediment administratiu comú de les administracions públiques, la Llei 40/2018 de règim jurídic del sector públic i el Reial decret 3/2010, pel qual es regula l'Esquema Nacional de Seguretat en l'àmbit de l'administració electrònica.

5. DADES DE CARÀCTER PERSONAL

La Universitat Politècnica de València tracta dades de caràcter personal, i aplica en aquest tractament les mesures de seguretat adequades tenint en compte l'estat de la tècnica, els costos d'aplicació i la naturalesa, l'abast, el context i les finalitats del tractament, així com els riscos de probabilitat i gravetat variables per als drets i les llibertats de les persones físiques.

Així mateix, s'aplicaran les mesures tècniques i organitzatives apropiades per a garantir un nivell de seguretat adequat al risc detectat, amb la finalitat d'assegurar la confidencialitat, la integritat, la disponibilitat i la resiliència permanents dels sistemes i serveis de tractament.

6. ORGANITZACIÓ DE LA SEGURETAT

6.1. ROLS: FUNCIONS I RESPONSABILITATS

6.1.1. La persona responsable de seguretat de la informació

té entre les seues funcions:

a) Mantenir la seguretat de la informació manejada i dels serveis prestats pels sistemes d'informació en el seu àmbit de responsabilitat, d'acord amb el que s'estableix en la política de seguretat de l'organització.
b) Promoure la formació i la conscienciació en

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

matèria de seguretat de la informació dins del seu àmbit de responsabilitat.
c) Participar en les anàlisis de risc, ajudant a determinar la categoria del sistema i establint la declaració d'aplicabilitat i les mesures de seguretat addicionals.
d) Acordar la suspensió del maneig d'una certa informació o la prestació d'un cert servei si se l'informa de deficiències greus de seguretat que puguen afectar la satisfacció dels requisits establits.

6.1.2. El Comitè de Seguretat TIC

Actua com a responsable de la informació a la Universitat Politècnica de València, i és el responsable d'establir els requisits de la informació en matèria de seguretat.

El Comitè de Seguretat TIC té el rol de responsable del servei a la Universitat, i té la potestat de determinar els nivells de seguretat dels serveis, atesos els requisits de seguretat de la informació i afegint els requisits de disponibilitat, accessibilitat, interoperabilitat, etc. necessaris.

El Comitè de Seguretat de la Informació no és un comitè tècnic, però recaptarà regularment del personal tècnic propi o extern la informació pertinent per a prendre decisions. El Comitè de Seguretat de la Informació s'assessorarà dels temes sobre els quals haja de decidir o emetre una opinió. Aquest assessorament es determinarà en cada cas, i es podrà materialitzar de diferents formes i maneres mitjançant:

a) Grups de treball especialitzats interns, externs o mixtos.
b) Assessoria externa.
c) Assistència a cursos o un altre tipus d'entorns formatius o d'intercanvi d'experiències

6.1.3. Prefectures de servei de l'àmbit competent en matèria TIC

Les persones que exerceixen les prefectures de

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

servei de l'àmbit competent en matèria TIC tenen la funció de responsables de sistemes.

Tenen com a responsabilitats:

a) Desenvolupar, operar i mantenir el sistema d'informació durant tot el seu cicle de vida, les seues especificacions, la instal·lació i la verificació del seu funcionament correcte.
b) Definir la topologia i sistema de gestió del sistema d'informació establint els criteris d'ús i els serveis disponibles en aquest.
c) Cerciorar-se que les mesures específiques de seguretat s'integren adequadament dins del marc general de seguretat.
d) Actuen com a administradores de la seguretat dels sistemes les persones amb el càrrec de cap de servei de l'àmbit competencial en matèria TIC. Entre les seues funcions hi ha:
d.1) La implementació, gestió i manteniment de les mesures de seguretat aplicables al sistema d'informació.
d.2) La gestió, configuració i actualització, si s'escau, del maquinari i programari en què es basen els mecanismes i serveis de seguretat del sistema d'informació.
d.3) La gestió de les autoritzacions concedides als usuaris i usuàries del sistema, en particular els privilegis concedits, inclòs el monitoratge que l'activitat desenvolupada en el sistema s'ajusta a allò autoritzat.
d.4) L'aplicació dels procediments operatius de seguretat.
d.5) Aprovar els canvis en la configuració vigent del sistema d'informació.
d.6) Assegurar que els controls de seguretat establits es compleixen estrictament.
d.7) Assegurar que s'apliquen els procediments aprovats per a manejar el sistema d'informació.
d.8) Supervisar les instal·lacions de maquinari i programari, i les seues modificacions i millores per a assegurar que la seguretat no està compromesa i que en tot moment s'ajusten a les autoritzacions pertinents.
d.9) Monitorar l'estat de seguretat del sistema proporcionat per les eines de gestió d'esdeveniments de seguretat i mecanismes

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.
d.9) Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría

d'auditoria tècnica implementats en el sistema.
d.10) Informar les persones responsables de la seguretat i del sistema de qualsevol anomalia, compromís o vulnerabilitat relacionada amb la seguretat.
d.11) Col·laborar en la investigació i resolució d'incidents de seguretat, des de la detecció fins a la resolució.

6.2. PROCEDIMIENTS DE DESIGNACIÓ

La persona responsable de la seguretat de la informació serà nomenada pel Rectorat a proposta del Comitè de Seguretat TIC. El nomenament es revisarà cada dos anys o quan el lloc quede vacant.

6.3. POLÍTICA DE SEGURETAT DE LA INFORMACIÓ

És missió del Comitè de Seguretat TIC la revisió anual d'aquesta política de seguretat de la informació i la proposta de revisió o manteniment d'aquesta.

La política serà aprovada pel Consell de Govern i es difondrà perquè la coneguen totes les parts afectades.

7. PREVENCIÓ

La Universitat Politècnica de València ha d'evitar o almenys prevenir en la mesura que siga possible, que la informació o els serveis es vegen afectats per incidents de seguretat. Per a això s'han d'implementar les mesures mínimes de seguretat determinades per l'ENS, així com qualsevol control addicional identificat a través d'una avaluació d'amenaces i riscos. Aquests controls, i els rols i responsabilitats de seguretat de tot el personal, han d'estar clarament definits i documentats.

Per a garantir el compliment d'aquesta política, la Universitat ha de:

a) Autoritzar els sistemes abans d'entrar en operació, aplicant els principis de seguretat des del disseny i per defecte.
b) Avaluar regularment la seguretat, incloent-hi

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 Responsable de Seguridad de la Información será nombrado por el rectorado a propuesta del Comité de Seguridad TIC. El nombramiento se revisará cada dos 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

avaluacions dels canvis de configuració fets de forma rutinària.
c) Sol·licitar la revisió periòdica per part de tercers amb la finalitat d'obtenir una avaluació independent.

8. DETECCIÓ

Atès que els serveis es poden degradar ràpidament a causa d'incidents, que van des d'una simple desacceleració fins a la seua detenció, els serveis han de monitorar l'operació de manera contínua per a detectar anomalies en els nivells de prestació dels serveis i actuar en conseqüència segons el que s'estableix en l'article 9 de l'Esquema Nacional de Seguretat.

El monitoratge és especialment rellevant quan s'estableixen línies de defensa d'acord amb l'article 8 de l'Esquema Nacional de Seguretat. S'establiran mecanismes de detecció, anàlisi i informe que arriben a les persones responsables regularment i quan es produeix una desviació significativa dels paràmetres que s'han preestablit com a normals.

9. RESPOSTA

La Universitat Politècnica de València ha de:

a) Establir mecanismes per a respondre eficaçment als incidents de seguretat.
b) Designar punt de contacte per a les comunicacions respecte a incidents detectats en altres departaments o en altres organismes.

c) Establir protocols per a l'intercanvi d'informació relacionada amb l'incident. Això inclou comunicacions, en tots dos sentits, amb els equips de resposta a emergències (CERT).

10. RECUPERACIÓ

Per a garantir la disponibilitat dels serveis crítics, l'organització ha de desenvolupar plans de continuïtat dels sistemes TIC com a part del seu pla general de continuïtat de negoci i activitats de recuperació.

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. GESTIÓ DE RISCOS

Tots els sistemes subjectes a aquesta política hauran de realitzar una anàlisi de riscos, i avaluar les amenaces i els riscos als quals estan exposats.

Aquesta anàlisi es durà a terme en els supòsits següents:

a) De forma regular, almenys una vegada cada dos anys.
b) En el cas que es canvie la informació manejada.

c) En el cas que canvien els serveis prestats.
d) Sempre que ocórrega un incident greu de seguretat.
e) En tot cas quan es reporten vulnerabilitats greus.

f) En qualsevol moment que siga necessari d'acord amb el que s'estableix en la normativa de protecció de dades personals.

Per a l'harmonització de les anàlisis de riscos, el Comitè de Seguretat TIC establirà una valoració de referència per als diferents tipus d'informació manejats i els diferents serveis prestats. El Comitè de Seguretat TIC dinamitzarà la disponibilitat de recursos per a atendre les necessitats de seguretat dels diferents sistemes, promovent inversions de caràcter horitzontal.

12. DESENVOLUPAMENT DE LA POLÍTICA DE SEGURETAT DE LA INFORMACIÓ

Aquesta política es desenvoluparà per mitjà de normativa de seguretat que afronte aspectes específics. La normativa de seguretat estarà a disposició de tots els membres de la Universitat Politècnica de València que necessiten conèixer-la, en particular, aquells que utilitzen, operen o administren els sistemes d'informació i comunicacions.

La normativa de seguretat estarà disponible en la intranet de la Universitat Politècnica de València.

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 llevara 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. OBLIGACIONS DEL PERSONAL

Tots els membres de la Universitat Politècnica de València tenen l'obligació de conèixer i complir aquesta política de seguretat de la informació i la normativa de seguretat, sent responsabilitat del Comitè de Seguretat TIC disposar els mitjans necessaris perquè la informació arribe a les persones afectades.

Tots els membres de la Universitat Politècnica de València assistiran a sessions de conscienciació en matèria de seguretat TIC. S'establirà un programa de conscienciació contínua per a atendre tots els membres d'aquesta, en particular els de nova incorporació.

Les persones amb responsabilitat en l'ús, operació o administració de sistemes TIC rebran formació per al maneig segur dels sistemes en la mesura que la necessiten per a fer el seu treball. La formació és obligatòria abans d'assumir una responsabilitat, tant si és la primera assignació com si es tracta d'un canvi de lloc de treball o de responsabilitats en aquest.

14. TERCERES PARTS

Quan la Universitat Politècnica de València preste serveis a altres organismes o faça servir informació d'altres organismes, se'ls farà partícips d'aquesta política de seguretat de la informació; s'establiran canals per a informes i coordinació dels respectius comitès de seguretat TIC, i s'establiran procediments d'actuació per a la reacció davant d'incidents de seguretat.

Quan la Universitat Politècnica de València utilitze serveis de tercers o cedisca informació a tercers, se'ls farà partícips d'aquesta política de seguretat i de la normativa de seguretat que concernisca a aquests serveis o informació. Aquesta tercera part quedarà subjecta a les obligacions establides en aquesta normativa, podent desenvolupar els seus propis procediments operatius per a satisfer-la. S'establiran procediments específics d'informe i resolució d'incidències. Es garantirà que el personal

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

de tercers està adequadament conscienciat en matèria de seguretat, almenys al mateix nivell que l'establit en aquesta política.

Quan algun aspecte de la política no puga ser satisfet per una tercera part (d'acord amb el que es requereix en els paràgrafs anteriors), es requerirà un informe de la persona responsable de seguretat a fi que precise els riscos en què s'incorre i la manera de tractar-los. Es requereix l'aprovació d'aquest informe per part de les persones responsables de la informació i els serveis afectats, abans de continuar avant.

15. ENTRADA EN VIGOR

a) Aquesta política de seguretat de la informació és efectiva des de l'aprovació pel Consell de Govern i fins que siga reemplaçada per una nova política.

b) Així mateix, aquesta política de seguretat de la informació serà publicada en el *Butlletí Oficial de la Universitat Politècnica de València* (BOUPV).

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.

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).