NORMATIVA DE SEGURIDAD DE LA UNIVERSITAT POLITÈCNICA DE VALÈNCIA

Aprobada por Consejo de Gobierno de 6 de junio de 2024

Contenido

CAPÍTULO I
DISPOSICIONES GENERALES

Artículo 1. Objeto

La presente normativa tiene por objeto regular la norma de uso seguro de los medios tecnológicos que forman parte de los sistemas de información de la Universitat Politècnica de València, con el fin de minimizar la probabilidad de la materialización de las amenazas que ponen en riesgo la seguridad de los sistemas de información.

Artículo 2. Definiciones

1. Sistemas de información: Conjunto de elementos (hardware, software, datos, procesos y personal) que permiten recopilar, almacenar, procesar y transmitir información para gestionar operaciones y tomar decisiones.
2. Recursos y servicios TIC: Recursos tecnológicos y servicios relacionados, como hardware, software, bases de datos, redes y servicios de telecomunicaciones, que se utilizan para respaldar y administrar sistemas de información.
3. Red Corporativa: Conjunto de redes y sistemas interconectados que permiten la comunicación y transmisión de datos entre diferentes áreas de una organización.
4. Correo electrónico corporativo: Sistema de comunicación por correo electrónico que pertenece a una organización y se utiliza para comunicaciones oficiales entre empleados y hacia otros agentes de interés.
5. Cookies: Archivos de datos pequeños almacenados en el dispositivo del usuario por un sitio web. Se utilizan para recordar información del usuario, como preferencias de navegación y detalles de inicio de sesión.
6. EDR (Endpoint Detection and Response): Herramientas y soluciones de seguridad diseñadas para detectar, analizar y responder a amenazas y actividades sospechosas en dispositivos finales (como ordenadores personales, ordenadores portátiles, servidores y dispositivos móviles).
7. Información clasificada: Información cuyo acceso está restringido a personas con autorización específica, generalmente por motivos de seguridad o confidencialidad.
8. Infraestructura de red: Conjunto de hardware, software y sistemas interconectados que forman la base para la comunicación y transmisión de datos en una red.
9. Sistemas físicos: Componentes tangibles de un sistema, como servidores, ordenadores personales, dispositivos de red y otros elementos de hardware.
10. Sistemas lógicos: Componentes intangibles de un sistema, como software, aplicaciones, bases de datos y algoritmos, que operan sobre sistemas físicos para gestionar datos y procesos.

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

Artículo 3. Ámbito de aplicación

1. Esta normativa es de obligado cumplimiento y se aplica a aquellas personas que tengan la consideración de usuarios de los recursos y servicios TIC de la Universitat Politècnica de València.

2. Tienen la consideración de usuarios:

a) Los miembros de la comunidad universitaria (PDI, PAS, PI y estudiantes).
b) El personal de las fundaciones y organizaciones dependientes de la Universitat Politècnica de València, siempre que tengan acceso a los recursos y servicios TIC de la Universitat Politècnica de València.
c) El personal de las organizaciones proveedoras de servicios, siempre que la prestación de sus servicios requiera el acceso a los recursos y servicios TIC de la Universitat Politècnica de València. Cuando este personal sea integrador de tecnología en el sistema, será obligatorio cumplir con normativas de usuarios avanzados.
d) Aquellas personas que, aunque no formen parte de ninguno de los colectivos anteriores, sean habilitadas para el uso de los recursos TIC de la Universitat Politècnica de València, siempre que se haya establecido un acuerdo de colaboración o una autorización explícita que así lo permita.

CAPÍTULO II.
USOS DE LOS RECURSOS Y SERVICIOS TIC

Artículo 4. Uso de los recursos TIC

1. La Universitat Politècnica de València pone a disposición de los usuarios de la comunidad universitaria conexiones a la red corporativa, las cuales se asignan a los usuarios en función de las características de la vinculación del usuario con la Universitat Politècnica de València.

2. El conjunto de servicios y recursos TIC que la Universitat Politècnica de València puede prestar y poner a disposición de los usuarios puede modificarse, o incluso terminar su prestación, en función de la disponibilidad de recursos y los cambios en la vinculación del usuario con la institución.

3. Los recursos y servicios TIC (dispositivos, programas, servicios informáticos, etc) que la Universitat Politècnica de València pone a disposición de los usuarios, deberán utilizarse fundamentalmente para el desarrollo de las funciones encomendadas, es decir, para fines profesionales o académicos.

4. Con carácter general, los equipos informáticos propiedad de la Universitat Politècnica de València los gestionará y configurará el personal técnico de la Universidad. Ningún usuario deberá realizar cambios en su configuración ni ejecutar o guardar archivos no confiables.

5. Los equipos propiedad de la Universitat Politècnica de València que sean transportados fuera de sus instalaciones deberán ser vigilados, y estar bajo control de los usuarios, asegurando un transporte seguro para evitar hurtos, extravíos o accesos no autorizados.

6. Todos los equipos que se conecten a la red de la Universitat Politècnica de València, deberán mantener el sistema operativo convenientemente actualizado para evitar vulnerabilidades y deben disponer del antivirus y sistema EDR oficiales de la Universitat Politècnica de València conveniente actualizados y operativos. No se podrán conectar a la red aquellos equipos informáticos cuyo sistema operativo esté fuera de soporte por su fabricante. Los equipos que se conecten a la red de la Universitat Politècnica de València desde fuera de los campus a través de la VPN deberán de cumplir igualmente con estos requisitos.

7. Cuando por razones justificadas un usuario tenga permisos para administrar ordenadores de la Universitat Politècnica de València, además de cumplir con lo dispuesto en el anterior apartado deberá asegurarse de instalar exclusivamente programas con licencia.

8. Cuando por razones justificadas un dispositivo deba tener habilitada cualquier tecnología que permita acceder directamente a dicho equipo desde internet, como el acceso web u otros, las aplicaciones de control remoto, o cualquier otro tipo de conexión remota por cualquier puerto de comunicaciones el procedimiento a seguir será el siguiente:

a) El administrador de dicho equipo debe justificar los motivos por los que es necesario dicho acceso desde internet mediante una declaración responsable en la que se especifiquen el propósito del equipo, los puertos a abrir y la tecnología que se va a utilizar, el tiempo de vigencia de dicha circunstancia excepcional y el compromiso de mantener el equipo permanente actualizado para evitar vulnerabilidades y de tener activado y actualizado permanentemente el sistema antivirus y el sistema EDR oficiales de la Universitat Politècnica de València.
b) El Área de Sistemas de Información y Comunicaciones (ASIC) a la vista del compromiso anteriormente descrito deberá autorizar la apertura de los puertos requeridos antes de que esta sea efectiva.
c) Cualquier incumplimiento de los compromisos asumidos en la declaración responsable implicará la desconexión inmediata del equipo de la red acordada por el responsable de seguridad de la información.

Artículo 5. Credenciales y contraseñas

1. La Universitat Politècnica de València proporcionará a los usuarios una cuenta de acceso consistente en credenciales, a través de la cual podrá utilizar los recursos y servicios TIC para los que haya sido habilitado. La finalización de la relación que vincula a los usuarios con la Universitat Politècnica de València comportará la finalización del derecho a utilizar los recursos y servicios TIC suministrados por la institución.

2. Las credenciales proporcionadas por la Universitat Politècnica de València a los usuarios serán personales e intransferibles, identificando inequívocamente al usuario.

3. Se prohíbe la comunicación de las contraseñas a terceras personas, tengan o no vinculación con la Universitat Politècnica de València. Su custodia y uso diligente es responsabilidad del usuario.

4. La Universitat Politècnica de València debe garantizar su inviolabilidad, de forma que sólo el titular pueda acceder a los recursos asociados a su cuenta, salvo en los casos y con las garantías en las que el ordenamiento jurídico lo permita.

5. El usuario procederá a cambiar las contraseñas cuando el sistema lo solicite y siempre utilizará contraseñas seguras.

Artículo 6. Impresión y digitalización de documentos

1. Con carácter general, deberán utilizarse impresoras en red y fotocopiadoras que sean propiedad de la organización y hayan sido autorizadas.

2. Toda digitalización deberá realizarse con los medios técnicos corporativos, evitando en todo momento hacer uso de dispositivos ajenos a la Universitat Politècnica de València, tales como fotografías con teléfonos móviles personales, etc.

3. Cuando se digitalice algún documento, deberá de atenderse con especial cuidado el destino de estos documentos.

4. Cuando se imprima documentación, deberá permanecer el menor tiempo posible en las bandejas de salida de las impresoras, para evitar que terceras personas puedan acceder a la misma.

5. Las fotocopias o copias desechadas no podrán ser reutilizadas cuando contengan datos personales o información clasificada, debiéndose proceder a su inmediata destrucción.

6. Queda prohibido dejar abandonados documentos con información clasificada en la impresora, fotocopiadora o dispositivos similares, o desatendida en el puesto de trabajo.

Artículo 7. Uso de la infraestructura de red

1. Los equipos informáticos de propiedad particular podrán conectarse a la red de la Universitat Politècnica de València tanto de forma inalámbrica como por cable. En el segundo caso deberán contar con la correspondiente autorización del o de la responsable de seguridad de la información

2. La conexión de los equipos informáticos particulares a la red de la Universitat Politècnica de València podrá restringirse o limitarse por motivos técnicos y para garantizar la seguridad.

3. No se permitirá la conexión de equipos mediante cable a la red de la Universitat Politècnica de València que no dispongan de persona de contacto o mecanismos que garanticen que en todo momento se pueda identificar a la persona que está utilizando el equipo.

4. No se permite poner en marcha infraestructuras o servicios, locales o remotos, que permitan el acceso a la red corporativa, usables por el usuario o por terceras personas, ni en abierto ni con acceso controlado, sin pedir autorización expresa del ASIC.

5. Los servicios informáticos de la universidad a través del personal técnico propio o de entidades proveedoras de servicios, es el único autorizado para acceder físicamente, administrar y manipular los sistemas de comunicaciones, cableado, puntos de acceso inalámbrico y cualquier otro equipamiento de la red.

6. Por motivos técnicos y para garantizar el buen funcionamiento de las comunicaciones en la red de la Universitat Politècnica de València, el personal técnico puede revertir cualquier actuación no autorizada realizada sobre cualquier elemento conectado a la red corporativa. Cualquier perjuicio generado por este tipo de actuaciones será responsabilidad del personal no autorizado que haya realizado tal acción.

Artículo 8. Puesto de trabajo despejado

1. En la medida de lo posible se deberá mantener el puesto de trabajo limpio, ordenado y despejado, sin más material encima de la mesa que el requerido para la actividad que se está realizando en cada momento.

2. La documentación, una vez usada, deberá almacenarse en un lugar cerrado, especialmente cuando el puesto de trabajo quede desatendido y al finalizar la jornada.

3. No estará permitido apuntar las contraseñas en post-it o similares y almacenarlas en el puesto de trabajo.

4. Cuando el usuario se ausente de su puesto de trabajo debe ser cauto y no mostrar en la pantalla documentos de trabajo.

5. En cada ordenador deberá estar activado el bloqueo automático de pantalla transcurrido un cierto tiempo de inactividad, con una validación de contraseña. Este bloqueo nunca deberá ser desactivado, siendo aconsejable bloquear manualmente la pantalla antes de abandonar el puesto por un tiempo prolongado, con el fin de que no se produzcan accesos indebidos.

6. En los ordenadores de uso compartido será obligatorio cerrar la sesión al abandonar el puesto.

7. Se considera un uso indebido la sustracción o el traslado no debidamente autorizado a otras dependencias, de cualquier elemento físico de la instalación informática o de la infraestructura complementaria, así como el causar daños a los mismos.

Artículo 9. Uso del correo electrónico

1. El correo electrónico corporativo es una herramienta de trabajo que deberá utilizarse para la realización de las funciones académicas, de investigación y administrativas propias de la Universidad. Se permite el uso en el ámbito privado cuando se trate de motivos personales o domésticos, que no sea abusivo y no perjudique la seguridad de los sistemas de información de la organización, ni el normal desarrollo de las funciones que se tengan encomendadas.

2. El usuario será responsable de las acciones realizadas a través de su cuenta de correo.

3. El personal técnico podrá acceder a los registros de uso de una cuenta de correo electrónico cuando dicho acceso sea necesario para garantizar la seguridad, disponibilidad, integridad y correcto funcionamiento de los recursos TIC.

4. Los usuarios deberán ser especialmente diligentes en la apertura de aquellos correos electrónicos que incorporen ficheros adjuntos y enlaces (URL), no debiendo abrir aquellos ficheros que provengan de fuentes no fiables ni enlaces de apariencia no legítima.

En caso de sospechas o dudas razonables sobre la confiabilidad de los ficheros y enlaces recibidos, deberán notificar esta circunstancia al ASIC a través del sistema de notificación de incidencias Gregal o a través de la cuenta de correo antifraude de la Universitat Politècnica de València: fraudeinternet@upv.es.

5. Se prohíbe el uso de la cuenta de correo electrónico corporativo para:

a) El envío de correos electrónicos con contenido inadecuado, ilegal, ofensivo, difamatorio, inapropiado o discriminatorio por razón de sexo, raza, edad, discapacidad, que contengan programas informáticos (software) sin licencia, que vulneren los derechos de propiedad intelectual de los mismos, de alerta de virus falsos o difusión de virus reales y código malicioso, o cualquier otro tipo de contenidos que puedan perjudicar a los usuarios, identidad e imagen corporativa y a los propios sistemas de información de la organización.
b) El envío de SPAM, correos masivos y propagación de correos encadenados.

c) El envío de mensajes relacionados con actividades ilegales o fraudulentas.
d) Cualquier otra que sea incompatible con las finalidades de la Universitat Politècnica de València y en general cualquier contravención de las finalidades contenidas en esta normativa o reglamento aplicable.

Artículo 10. Protección de la navegación web

1. La utilización de internet deberá limitarse a la obtención de información relacionada con el trabajo que se desempeña, debiendo por lo tanto evitarse toda utilización que no tenga una mínima relación con las funciones encomendadas al usuario.

2. No estará permitido el acceso a páginas de contenido ofensivo, inapropiado, pornográfico, o discriminatorio por razones de género, etnia, opción sexual, discapacidad o cualquier otra circunstancia personal o social excepto por razones justificadas de investigación o docencia y siempre con la debida autorización del responsable de seguridad de la información.

3. El uso de páginas web debe ser a través del protocolo seguro HTTPS. Solo se permitirán los accesos mediante el protocolo HTTP no seguro en aquellos servicios que por motivos técnicos no ofrecen un medio seguro de conexión, teniendo la precaución de no transmitir datos personales ni información clasificada a través de este tipo de conexiones no seguras.

4. Los usuarios deberán verificar que los certificados remitidos por servicios HTTPS han sido remitidos por una Autoridad de Certificación de confianza. Cualquier error o alerta generada por el navegador como consecuencia de la validación del certificado deberá revisarse cuidadosamente con el fin de comprobar su licitud.

5. Con el fin de reducir la exposición a las cookies, se utilizarán perfiles de usuarios diferenciados en los navegadores web para separar las actividades relacionadas con la organización de las personales.

Artículo 11. Uso de las instalaciones técnicas

1. El acceso físico a áreas restringidas sólo se permitirá al personal autorizado, excepto en los supuestos de urgencia o emergencia.

2. El acceso a los Centros de Procesamiento de Datos (CPD) así como a las infraestructuras de comunicaciones de la Universitat Politècnica de València estará restringido al personal de los servicios informáticos de la Universitat Politècnica de València y al personal autorizado.

3. En caso de ser necesario el acceso a un CPD o a la infraestructura de comunicaciones por parte de personal no miembro de los servicios informáticos de la Universidad, el responsable de la visita formalizará la solicitud de autorización para este acceso.

4. Los accesos a los CPDs deben tener control de acceso y deberán registrarse los accesos.

Artículo 12. Uso indebido de los recursos TIC

Se considerará uso indebido de los recursos TIC y en ningún caso se podrán utilizar para ninguna de las siguientes finalidades:

a) Incurrir en actividades ilícitas o ilegales de cualquier tipo y, particularmente, difundir contenidos de carácter racista, xenófobo, pornográfico, sexista, de apología del terrorismo, que atenten contra los derechos humanos, o que actúen en perjuicio de los derechos a la intimidad, el honor, la propia imagen o contra la dignidad de las personas.
b) Difundir contenidos contrarios a los principios inspiradores de los Estatutos de la Universitat Politècnica de València.
c) Congestionar intencionadamente la red de la Universitat Politècnica de València o interferir en su funcionamiento.
d) Establecer mecanismos o sistemas que permitan aprovechamientos indebidos de los recursos de red proporcionados, como revenderlos o reutilizarlos para fines privados, lucrativos o delictivos, entre otros.
e) Dañar los sistemas físicos y lógicos, introducir o difundir en la red virus informáticos o software dañino y realizar cualquier otro tipo de actividad que sea susceptible de provocar daños en la Universitat Politècnica de València, a sus miembros, proveedores o terceras personas.
f) Recoger datos personales, tanto de forma directa como mediante tratamientos invisibles, excepto aquellos que estén directamente relacionados con las funciones propias de la Universidad, o realizar cualquier tratamiento de datos personales que no sean titularidad de la Universitat Politècnica de València y no haya sido previamente autorizado.
g) Instalar software para el que no se disponga de licencia, ni ejecutar o guardar archivos no confiables.
h) Publicar o difundir datos, documentos o archivos que afecten a terceras personas o que estén sujetos a derechos de privacidad en la protección de datos y garantía de los derechos digitales o de propiedad intelectual, así como a cualesquiera otros derechos o intereses legítimos, sin el consentimiento expreso de las personas afectadas y del titular de los derechos
i) Hacer uso de los recursos TIC con fines comerciales, salvo los casos autorizados expresamente.
j) Enviar comunicaciones con fines comerciales o correo masivo no solicitado con fines publicitarias (SPAM) desde las cuentas de correo electrónico.
k) Vulnerar los derechos de propiedad intelectual o industrial de terceros.
l) Buscar o utilizar identificadores y contraseñas de otros usuarios o cualquier intento de encontrar y explotar fallos en la seguridad de los sistemas informáticos de la Universidad o de fuera, o hacer uso de los sistemas para atacar cualquier sistema informático.

CAPÍTULO III
TRATAMIENTO DE LA INFORMACIÓN

Artículo 13. Clasificación de la información

La Universitat Politècnica de València pondrá a disposición de los usuarios un procedimiento de clasificación de información que debe utilizarse para el desarrollo de las funciones encomendadas.

Artículo 14. Manejo y tratamiento de la Información

1. Los usuarios tienen el deber de guardar la confidencialidad debida, de conformidad con la legislación vigente, respecto de la información manejada. Este deber de confidencialidad se extiende incluso una vez finalizada la relación del usuario con la Universitat Politècnica de València.

2. En caso de que se disponga de información en soporte papel, se deberá conservar y custodiar con la debida diligencia.

3. Las copias, extractos y traducciones estarán sujetos y deberán manejarse con los mismos requisitos de seguridad que los originales, pudiendo ser realizadas por usuarios con acceso autorizado a la información.

4. Queda expresamente prohibido el intercambio de información clasificada mediante plataformas no corporativas o no autorizadas.

5. Los archivos o ficheros clasificados por la Universitat Politècnica de València no se podrán utilizar para uso particular o de terceros. Durante el periodo de tiempo que los ficheros o archivos permanezcan en el equipo o soporte informático de su propiedad, se deberá restringir el acceso y uso de la información que obra en los mismos.

6. No se deberá copiar o enviar la información contenida en los ficheros en los que se almacenen datos de carácter personal u otro tipo de información de la Universitat Politècnica de València en ordenadores propios, pendrives, discos extraíbles o cualquier otro soporte informático.

7. En caso de que así fuera necesario, los archivos o ficheros clasificados por la Universitat Politècnica de València serán eliminados una vez que hayan dejado de ser útiles para los fines que motivaron su creación.

8. Antes de abandonar salas de uso común, se limpiarán adecuadamente las pizarras de las salas de reuniones o despachos, cuidando que no quede ningún tipo de información clasificada o que pudiera ser reutilizada.

Artículo 15. Almacenamiento de la Información

1. La información solamente podrá ser almacenada en recursos oficiales, como la unidad de red individual (W:), la unidad de red compartida con el servicio (V:), el servicio de OneDrive corporativo, así como en aquellos otros que autorice expresamente la Universitat Politècnica de València.

2. El usuario será el responsable de toda la información que haya almacenado y que sea extraída fuera de la Universitat Politècnica de València.

CAPITULO IV
RÉGIMEN DE VIGILANCIA Y RESPONSABILIDAD

Artículo 16. Responsabilidad de los usuarios

1. Los usuarios deben custodiar, y hacer un buen uso, de los recursos TIC que la Universitat Politècnica de València ponga a su disposición para desarrollar sus funciones dentro de la institución.

2. Cada usuario será responsable de las acciones realizadas a través de su cuenta y de los recursos TIC puestos a su disposición.

3. Ante el incumplimiento del deber de custodia de la cuenta, la Universitat Politècnica de València podrá iniciar un procedimiento administrativo para asegurar el correcto funcionamiento de los servicios prestados y adoptar las medidas correctoras y disciplinarias necesarias, entre ellas el bloqueo temporal de la cuenta de usuario como medida provisional.

4. Los usuarios tendrán la obligación de conocer y cumplir esta normativa y cualquier otra norma o instrucción que pueda afectar al uso correcto de las TIC, tanto en la Universitat Politècnica de València, como en aquellas redes de las que la Universidad forme parte.

5. La Universitat Politècnica de València no es responsable, directa ni subsidiariamente, de las opiniones expresadas por los miembros de la comunidad universitaria o por cualesquiera otros, ni de los contenidos publicados en los recursos de debate público online proporcionados por la institución.

Artículo 17. Incidentes de seguridad

Cuando un usuario detecte cualquier anomalía o incidencia de seguridad que pueda comprometer el buen uso y funcionamiento de las instalaciones o de los Sistemas de Información de la Universitat Politècnica de València, deberá informar inmediatamente a través del sistema Gregal o del procedimiento que tenga a su disposición en ese momento en caso de urgencia.

Artículo 18. Análisis y monitorización de seguridad

1. La Universitat Politècnica de València, por motivos legales, de seguridad y calidad del servicio, y cumpliendo con los requisitos que le afectan por las legislaciones, cuenta con un sistema de ciberseguridad que monitorizan el estado del SGSI (Sistema de Gestión de la Seguridad de la Información), por lo que:

a) Revisará periódicamente el estado de los equipos, el software instalado, los dispositivos y redes de comunicaciones de su responsabilidad.

b) Monitorizará los accesos a la información y redes contenida en sus sistemas.

c) Auditará la seguridad de las credenciales y aplicaciones.

d) Monitorizará los servicios de internet, correo electrónico y otras herramientas de colaboración.

2.La Universitat Politècnica de València llevará a cabo estas actividades de monitorización de manera proporcional al riesgo, con las cautelas legales pertinentes con pleno respeto de los derechos de los usuarios.

3. El sistema que proporciona el servicio de navegación podrá contar con filtros de acceso que bloqueen el acceso a páginas web con contenidos inadecuados, programas lúdicos de descarga masiva o páginas potencialmente inseguras o que contengan virus o código dañino. Igualmente, el sistema podrá registrar y dejar traza de las páginas a las que se ha accedido, así como del tiempo de acceso, volumen y tamaño de los archivos descargados.

4. La Universitat Politècnica de València podrá suspender el uso de los recursos a los usuarios, temporal o definitivamente, cuando se detecte un uso inadecuado o se incumplan las directrices de seguridad para garantizar la seguridad de los sistemas de información.

Artículo 19. Incumplimiento de la Normativa

1. Los sistemas de la Universitat Politècnica de València se configurarán para prevenir acciones que puedan ser consideradas contrarias a este reglamento o en cualquier otra norma o protocolo aprobado. Estos sistemas podrán adoptar las medidas preventivas correspondientes.

2. El Responsable de Seguridad, en el ejercicio de sus funciones, ante un posible incumplimiento de la presente normativa que pueda suponer un perjuicio para los sistemas y recursos de la Universitat Politècnica de València, podrá proceder a la suspensión cautelar del servicio prestado o el bloqueo temporal de los sistemas, cuentas o accesos a la red de forma preventiva, con el fin de garantizar el buen funcionamiento de los servicios de la institución.

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

2. En los demás supuestos de incumplimiento, se advertirá del hecho al infractor. En caso de que el usuario no responda o ignore la advertencia, el Comité de Seguridad de la Información de la Universitat Politècnica de València podrá solicitar al Rector, o Vicerrector en quien éste haya delegado, la adopción de las medidas de suspensión provisional de los servicios prestados o bloqueo de los sistemas.

Todo ello sin perjuicio de iniciar las acciones disciplinarias, administrativas, civiles o penales que en su caso correspondan, en relación con las personas presuntamente implicadas en dicho incumplimiento.

La Universitat Politècnica de València pondrá en conocimiento de la autoridad judicial y las Fuerzas y Cuerpos de Seguridad del Estado aquellas infracciones que pueden ser constitutivas de delito.

Artículo 20. Revisión y evaluación

El Comité de Seguridad será competente para:

a) Interpretar las dudas que puedan surgir en la aplicación de esta normativa.
b) Proceder a la revisión de la normativa, cuando sea necesario para actualizar su contenido o se cumplan los plazos máximos establecidos para ello.
c) Verificar la efectividad de las medidas adoptadas por razón de esta normativa.

Anualmente, el presente documento se someterá a revisión y aprobación, de existir modificaciones en el mismo.

La modificación y su revisión, se orientará, tanto a la identificación de oportunidades de mejora en la gestión de la seguridad de la información, como a la adaptación a los cambios habidos en el marco legal, infraestructura tecnológica, organización general, etc.

2. El Responsable de Seguridad de la Información será la persona encargada de la difusión de la información y de las directrices incorporadas en esta normativa.

Disposición derogatoria única.

Queda derogado el Reglamento de Uso de los Servicios y Recursos Informáticos de la Universitat Politècnica de València de fecha 17 de mayo de 2007 y cualquier otra norma que la contravenga.

Disposición final única.

Esta Normativa entrará en vigor el mismo día de su publicación en el BOUPV.

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