Normativa de Seguridad y uso de los recursos informáticos en la Universidad Politécnica de Cartagena

El Consejo de Gobierno, en su sesión de 17 de diciembre de 2020, en virtud de lo dispuesto en el artículo 36 de los Estatutos aprobados por Decreto 1 / 2020 de 16 de enero del Consejo de Gobierno de la Comunidad Autónoma de la Región de Murcia (BORM de 5 de febrero de 2020) aprobó la presente normativa:

PREÁMBULO

La Política de Seguridad de la Universidad Politécnica de Cartagena (en adelante UPCT) supone un marco general sobre el tratamiento de la seguridad de la información en el ámbito de la Universidad que debe ser desarrollado con normativas más específicas. La presente normativa desarrolla lo expuesto en la Política de Seguridad de la UPCT sobre el uso correcto de los sistemas de información, así como un conjunto de buenas prácticas necesarias para la prevención, detección, respuesta y recuperación ante incidentes de seguridad.

La UPCT da una importancia estratégica al uso de las Tecnologías de la Información en general y de la red de datos en particular para fines investigadores, docentes y administrativos. Sin embargo, se trata de un recurso limitado y expuesto a amenazas y ataques, por lo que la UPCT se reserva el derecho a denegar el acceso a su infraestructura y servicios de red a aquellas personas, empresas u organismos que no se adecúen a las normas expuestas en este documento o que incumplan su Política de Seguridad.

Los usuarios de la red y de los servicios informáticos de la UPCT deben mantener la integridad de los recursos basados en los sistemas de información, evitar actividades destinadas a obtener accesos no autorizados o suplantación de identidad, respetar los derechos del resto de usuarios, no acaparar los recursos compartidos con el resto de usuarios, respetar las políticas de licencias de software y colaborar en evitar, identificar y resolver los incidentes de seguridad por los que se puedan ver afectados.

Esta normativa se debe aplicar a la red de la UPCT, a todos los equipos conectados a ella y a la información contenida en estos equipos.

En el ámbito de la presente Normativa, se utiliza el término “Recurso TIC” para referirse a cualquier dispositivo, infraestructura, instalación, servicio o aplicación informática que dé cobertura al uso de las tecnologías de la información y las comunicaciones de apoyo a la gestión de los servicios y procedimientos y la información de la que es responsable la UPCT.

La definición de esta Normativa corresponde al Comité de Seguridad TIC, que es competente para:

- Interpretar las dudas que puedan surgir en su aplicación.
- Proceder a su revisión, cuando sea necesario para actualizar su contenido o se cumplan los plazos máximos establecidos para ello.
- Verificar su efectividad.

El Responsable de Seguridad y el Responsable del Sistema ejercerán las funciones y responsabilidades definidas en la Política de Seguridad de la UPCT. Será el Responsable de Seguridad la persona encargada del mantenimiento actualizado de la Normativa de Seguridad y de su divulgación.
Esta normativa se ha desarrollado teniendo como referencia las pautas y el modelo especificado en la Guía CCN-STIC 821 (sobre normas de seguridad) y las normativas de otras universidades de referencia.

ÍNDICE

TÍTULO I
DISPOSICIONES GENERALES

Artículo 1. Objeto

Esta normativa se basa en el cumplimiento de un conjunto de buenas prácticas de seguridad que ayudarán a proteger el conjunto de la información e infraestructura de la UPCT, interfiriendo lo menos posible con las actividades propias del entorno universitario. Se pretende también evitar el uso y abuso de los recursos TIC por parte de individuos o grupos no autorizados.

Artículo 2. Ámbito de aplicación

1. Lo expuesto en este documento se aplicará a todos los dispositivos conectados a la red de la UPCT o con direccionamiento IP dentro del rango asignado a la UPCT, tales como PCs, portátiles, impresoras, dispositivos móviles o servidores. También se aplicará a aquellos dispositivos no pertenecientes a la UPCT pero que se conecten a la misma, indistintamente de la tecnología de conexión utilizada.
2. Esta normativa es de aplicación a aquellas personas que tienen la consideración de usuarios de los recursos TIC de la UPCT o que disponen de una cuenta de usuario en el sistema de gestión de identidades de la UPCT. Tienen la consideración de usuarios:
    a. Los miembros de la comunidad universitaria (PDI, PAS y estudiantes).
    b. El personal de las fundaciones y organizaciones dependientes de la UPCT y entidades colaboradoras, siempre que tengan acceso a los recursos y servicios TIC de la UPCT.
    c. El personal de las organizaciones proveedoras de servicios en la UPCT, siempre que la prestación de sus servicios requiera el acceso a los recursos y servicios TIC de la UPCT.
    d. Aquellas personas físicas o jurídicas que, a pesar de no formar parte de ninguno de los colectivos anteriores, sean habilitadas para el uso de los recursos TIC de la UPCT, para lo cual será necesaria una autorización explícita que así lo permita y les someta al cumplimiento de la Política de Seguridad de la UPCT y de la presente normativa.
3. Esta normativa también será de aplicación a los dispositivos que se conecten remotamente a la red de la UPCT para tareas relacionadas con la actividad universitaria.
4. Cuando sea necesario el uso de infraestructuras de red externas (como es el caso de la Red CTNet y RedIris), las políticas y recomendaciones de uso de estas instituciones serán de aplicación en la red de la UPCT.

TÍTULO II. USO SEGURO DE LOS SISTEMAS

Artículo 3. Sobre las cuentas de usuario: identificación y autenticación

1. Los usuarios dispondrán de una cuenta de usuario que consistirá en un identificador único y unas credenciales de acceso que permitan comprobar su identidad de forma segura en el acceso a los recursos TIC para los que hayan sido autorizados.
2. La finalización de la relación con la UPCT comporta la finalización del derecho a utilizar los recursos y servicios TIC suministrados por la institución. No obstante, la Universidad permitirá al usuario un periodo de tiempo para el acceso a sus datos con el fin de obtener copia antes de la cancelación de la cuenta de usuario siempre que ello no suponga una amenaza para la información y los recursos TIC responsabilidad de la Universidad. Del mismo modo, la UPCT, a través del Comité de Seguridad TIC, se reserva la posibilidad de poder ampliar el periodo de utilización de los recursos TIC a los usuarios una vez finalizada su vinculación con la institución.
3. Los privilegios de acceso deben ser los imprescindibles para la realización de las tareas encomendadas al puesto de trabajo; en caso de que el usuario observe que dispone de privilegios adicionales a los necesarios, lo debe notificar al Responsable del Sistema.
4. Los usuarios son responsables de la custodia de sus credenciales y de toda actividad relacionada con el usuario asignado. El identificador de usuario es único para cada persona en la organización e intransferible.
5. Los usuarios no deben revelar o entregar, bajo ningún concepto, sus credenciales a otra persona, ni mantenerlas por escrito a la vista o al alcance de terceros.
6. Los usuarios no deben utilizar ningún acceso autorizado de otro usuario, aunque dispongan de la autorización de su titular.
7. Si un usuario tiene sospechas de que sus credenciales están siendo utilizadas por otra persona o, de forma accidental, la ha proporcionado por un medio indebido, debe cambiarla inmediatamente y proceder a comunicar a la Unidad de Informática la correspondiente incidencia de seguridad. En la medida de lo posible, los sistemas alertarán al usuario de la fecha y hora de último acceso y en caso de detectarse cualquier inconsistencia al respecto el usuario es responsable de ponerlo en conocimiento a la Unidad de Informática.
8. El incumplimiento del deber de custodia de la cuenta supone una vulneración grave en la seguridad de la información. En su caso, la UPCT podrá iniciar un procedimiento disciplinario y adoptar las medidas

correctoras y disciplinarias necesarias, entre las cuales está el bloqueo inmediato de la cuenta de usuario como medida cautelar.

9. Se definirán y aprobarán unas instrucciones sobre contraseñas, que marcarán las directrices que deben seguir para ser suficientemente seguras: longitud, formato, restricciones y periodo de caducidad. Todas las contraseñas deberán cumplir los requisitos mínimos establecidos.

Artículo 4. Sobre el uso de los equipos informáticos

1. Los equipos informáticos y dispositivos de comunicaciones, tanto fijos como móviles, y la información, programas y otros servicios informáticos proporcionados a los usuarios para el desarrollo de su actividad profesional o docente deben utilizarse exclusivamente para el desarrollo de las funciones encomendadas.
2. Cualquier uso de los recursos informáticos se someterá a lo que especifica esta normativa en cuanto a monitorización y control (tal y como se especifica en el artículo 14 de esta normativa), debido a que dichos recursos son un elemento muy importante en la cadena de seguridad de los sistemas de información.
3. Como norma general, los equipos informáticos propiedad de la UPCT se instalan y configuran bajo la supervisión y/o directrices del personal técnico de la Unidad de Informática de la UPCT. Siguiendo el principio de “mínimos privilegios” se debe limitar en la medida de lo posible la capacidad de que el usuario pueda realizar cambios en su configuración.
4. Cuando por razones justificadas un usuario tenga permisos para administrar un equipo informático propiedad de la UPCT, este será responsable:
    a. De mantener actualizada la seguridad de los sistemas operativos, antivirus y cortafuegos (firewalls) mediante actualizaciones automáticas de seguridad pudiendo contar con la asistencia de la Sección de Soporte de la Unidad de Informática.
    b. De instalar únicamente programas para los cuales la UPCT tiene licencia de uso, bien porque sea software libre o porque se haya adquirido. No se permite instalar software para el cual no se disponga de licencia, ni ejecutar o guardar archivos no confiables.
5. Los usuarios deberán facilitar al personal de soporte técnico el acceso a sus equipos informáticos propiedad de la Universidad para labores de reparación, instalación o mantenimiento. Si el personal de soporte técnico detectase cualquier anomalía que indicara una utilización de los recursos contraria a la presente norma, lo pondrá en conocimiento del Responsable de Seguridad y/o del Responsable del Sistema, que tomarán las oportunas medidas correctoras.

6. La responsabilidad del uso adecuado de las herramientas informáticas, como el equipo personal, los periféricos y los programas instalados, es del propio usuario. El usuario de equipos informáticos debe procurarse los conocimientos imprescindibles para el manejo seguro y buen uso de los sistemas de información. La UPCT pondrá a disposición de los usuarios herramientas que les facilitarán realización de copias de seguridad de los datos que consideren relevantes. La UPCT realiza copias de seguridad de los datos y ficheros almacenados en los espacios de almacenamiento corporativos.
7. Sólo está permitida la conexión a la red cableada de la UPCT de equipos informáticos inventariados en la propia Universidad. De forma excepcional se podrá permitir la conexión de otros equipos, con una duración limitada en el tiempo, siempre que esté debidamente justificada; la autorización corresponderá al Responsable de Seguridad de la UPCT y/o del Responsable del Sistema.
8. Se permite la conexión de equipos informáticos de propiedad particular a la red inalámbrica de la universidad (red eduroam), siempre que se cumpla esta normativa y el resto de instrucciones que la desarrollen.
9. En cualquier caso, a continuación, se plantean los aspectos mínimos de seguridad que deben ser tenidos en cuenta por todos los usuarios:
    a. Actualizaciones del Sistema Operativo: Los equipos conectados a la red UPCT deben estar al día en cuanto a las actualizaciones del Sistema Operativo, especialmente, las de seguridad; la única excepción será para los casos de no compatibilidad con aplicaciones necesarias para el trabajo del usuario en cuyo caso lo pondrán en conocimiento del Responsable de Seguridad o el Responsable del Sistema para que tomen las medidas oportunas.
    b. Antivirus: Todos los equipos deben tener activo y actualizado un software antivirus o de protección del equipo, preferentemente facilitado bajo licencia corporativa por la UPCT.
    c. Inventariado y trazabilidad: los equipos de usuario, propiedad de la UPCT, deben tener instalado un software que permita disponer de un inventario automatizado y la monitorización de configuraciones y eventos básicos del sistema.
    d. Protección del equipo por inactividad: El equipo o puesto de trabajo se deberá configurar para que se bloquee al cabo de un tiempo prudencial de inactividad, requiriendo una nueva autenticación del usuario para reanudar la actividad en curso.
    e. Servicios o aplicaciones no necesarias: Los equipos informáticos deberán contar con los servicios y aplicaciones mínimas necesarias para el desarrollo de las funciones desempeñadas por el usuario. Si una aplicación no es necesaria para el trabajo del usuario del equipo,

no debe estar instalada y desde la Unidad de Informática se podrá requerir al usuario la desinstalación de esta.

f. El uso del software instalado en equipos informáticos de la Universidad debe ajustarse a la normativa legal vigente. En consecuencia, los usuarios deben asegurarse de que disponen de las licencias adecuadas al uso que hagan de dicho software, ya sea mediante licencias adquiridas de forma centralizada por la UPCT (para software de uso común) o bien la adquisición de las correspondientes licencias, o bien el uso de software libre. De no ser así la responsabilidad recaerá totalmente sobre el usuario.

10. En caso de robo o extravío del equipo se debe comunicar inmediatamente a la Gerencia de la Universidad.

Artículo 5. Sobre gestión y acceso a la Red de la UPCT

1. La Unidad de Informática de la UPCT, a través de personal propio o de proveedores de servicios, es la responsable única de la administración y gestión de la Red de la Universidad:
    a) La instalación (o cambios) de nuevos puntos de red conectados a la Red de la UPCT se hará de conformidad con los criterios aprobados (según la instrucción técnica de aplicación) y será competencia exclusiva de la Unidad de Informática.
    b) No se permitirá la instalación de electrónica de red (conmutadores, hubs, routers) y de puntos de acceso de redes inalámbricas con conexión a la Red de la UPCT sin la debida autorización de la Unidad de Informática. En caso de detección de algún equipo no autorizado se procederá a su inmediata desconexión.
    c) Los equipos electrónicos de gestión e infraestructura de la red de la UPCT serán instalados, configurados y mantenidos exclusivamente por la Unidad de Informática.
    d) No se permite el empleo de mecanismos para la manipulación de direcciones de red o cualquier otro uso que pueda afectar a la topología o a la estructura lógica de la red de la UPCT.

2. Todos los equipos que se conectan a la red deben recibir una dirección IP y un nombre de red asignados por la Unidad de Informática, además de ser incluidos en el registro correspondiente, junto con la identidad y los datos de contacto del responsable del equipo. No está permitida la conexión de equipos con direcciones no registradas.

3. En el caso de los servidores departamentales, o sea, aquellos instalados en un departamento y administrados por personal del mismo para dar un determinado servicio propio del departamento, debe quedar claramente definida la persona que actúa como responsable del mismo y quién se encarga de su mantenimiento, además de la información técnica oportuna según se indique en la instrucción específica que se desarrolle al efecto. Esta persona deberá responder ante incidencias e incumplimiento de esta Normativa por parte del sistema local.
4. La red de la UPCT sólo tendrá un enlace con Internet (a través de la infraestructura proporcionada por RedIris) cuya administración y correcto funcionamiento es responsabilidad de la Unidad de Informática.
5. Los usuarios de la red no deben utilizar esta infraestructura y servicios para otros usos que no sean los permitidos en la Política de uso de RedIRIS (publicada en el portal web de RedIRIS) o los propios necesarios para el desempeño de su actividad.
6. No está permitido que los usuarios utilicen su conexión a red para proporcionar acceso a terceras personas o entidades.
7. Ningún usuario está autorizado a utilizar analizadores del tráfico que circula por la red de la UPCT. Igualmente está prohibido utilizar herramientas de rastreo de puertos o que permitan detectar vulnerabilidades. El uso de estas herramientas sólo está permitido a los administradores de la red.
8. La actuación del personal técnico de la Unidad de Informática, encargado de la gestión y acceso a la red de la UPCT, se rige por los principios de profesionalidad, seguridad, secreto y pleno respeto de los derechos de los usuarios.

Artículo 6. Sobre seguridad en los accesos remotos para actividad no presencial

1. Se han de tener en cuenta una serie de pautas que permitan garantizar la seguridad de todas las herramientas y soluciones utilizadas en las actividades no presenciales (teletrabajo, docencia y evaluación on-line) y, de este modo, seguir manteniendo la confidencialidad, integridad, autenticidad, trazabilidad y disponibilidad, como si se estuviese en el propio puesto de trabajo físico.
2. En este sentido será de importancia primordial considerar las siguientes medidas básicas de protección de los equipos remotos y las conexiones:
    a. Los accesos remotos a equipos de la red de la Universidad solo se permitirán a través de conexiones seguras basadas en criptografía que serán facilitadas por la Unidad de Informática.

   b. Se podrán requerir mecanismos de autenticación de mayor nivel de seguridad que los empleados en los accesos desde dentro de la red de la Universidad.
   c. Los dispositivos remotos deberán disponer de un software antivirus activo y actualizado.
   d. Los dispositivos remotos deben estar al día en cuanto a las actualizaciones de seguridad del Sistema Operativo.
   e. La red doméstica desde la que se conecta el usuario debe reunir unas condiciones básicas de seguridad.
   f. Las conexiones a la red interna de la Universidad serán monitorizadas, en previsión para evitar riesgos y detectar posibles ataques.
3. En cualquier caso, los usuarios deben ser informados de cómo deben actuar cuando trabajan en remoto y de cómo deben crear un “entorno seguro” de teletrabajo.
4. Este artículo se desarrollará en una instrucción o guía de buenas prácticas para teletrabajo seguro.

Artículo 7. Sobre el uso del correo electrónico

1. El correo electrónico corporativo es un servicio de mensajería electrónica centralizada, puesto a disposición de los usuarios de la UPCT, para el envío y recepción de mensajes mediante el uso de cuentas de correo corporativas.
2. Todos los usuarios que lo precisen para el desempeño de su actividad universitaria dispondrán de una cuenta de correo electrónico, para el envío y recepción de mensajes internos y externos a la Universidad.
3. El usuario es responsable de las acciones realizadas mediante su cuenta de correo.
4. El uso principal de las cuentas de correo electrónico proporcionadas por la UPCT se tiene que relacionar con las finalidades de la Universidad, establecidas en las normas y en los Estatutos. Se permite la utilización privada de la cuenta de correo electrónico, siempre que este uso sea limitado y no impida la realización de su finalidad principal.
5. Las direcciones de correo electrónico de contacto del personal de la UPCT son públicas y pueden ser difundidas en directorios que tienen que contener indicación clara de las finalidades de tales direcciones. Se puede excluir o sustituir la dirección de correo electrónico de las listas públicas cuando haya causa justificada, y tengan que prevalecer los intereses o derechos de la persona afectada. La publicación de las cuentas de correo se protegerá de su extracción masiva para evitar un uso indebido de las mismas.

6. La Universidad no asume ninguna responsabilidad en los casos en que el usuario haya redireccionado el correo de la UPCT a una cuenta externa de correo electrónico.
7. Para verificación y monitorización, los datos de conexión y tráfico se guardarán en un registro durante el tiempo que establezca la normativa vigente en cada supuesto y podrán ser utilizados en caso de ser requerida la investigación de un incidente de seguridad o para la identificación de posibles mejoras de seguridad. En ningún caso esta retención de datos afectará al secreto de las comunicaciones.
8. Se definirá y aprobará una normativa específica de uso del correo electrónico, que desarrollará lo especificado en el presente texto.

Artículo 8. Protección de datos personales y deber de confidencialidad

1. La información contenida en las bases de datos de la UPCT que comprenda datos de carácter personal está sometida a la normativa vigente aplicable en materia de protección de datos personales. Los tratamientos de datos personales gestionados por la UPCT han de adoptar las medidas de seguridad que se correspondan con las exigencias previstas o derivadas de la antedicha normativa.
2. La UPCT dispone de una Política de Privacidad publicada en UPCTLex a la cual se somete cualquier tratamiento de datos personales responsabilidad de la Universidad.
3. La UPCT cuenta con un Delegado de Protección de Datos encargado de asesorar a la Universidad y a sus usuarios en el cumplimiento de la normativa aplicable en materia de protección de datos personales. Cualquier aspecto relacionado con el tratamiento de datos personales debe ser puesto en conocimiento del Delegado a través de los canales establecidos al efecto.
4. Todo usuario (de la UPCT o de terceras organizaciones) que, en virtud de su actividad profesional o académica, pudiera tener acceso a datos de carácter personal, está obligado a guardar la confidencialidad debida sobre los mismos; deber que se mantendrá de manera indefinida, incluso más allá de la relación con la UPCT.
5. Cuando así se requiera, los datos y la información sensible, confidencial o protegida, deberán ser eliminados de forma segura para evitar accesos ulteriores según el procedimiento que se establezca al efecto.

Artículo 9. Debate público en línea y recursos web bajo dominios UPCT.ES

1. La UPCT proporciona recursos de debate público e información en línea para la comunidad universitaria. La UPCT no es responsable, directamente ni subsidiariamente, de las opiniones expresadas por los miembros de la comunidad universitaria o por cualesquiera otros, ni de los contenidos publicados.
2. Los recursos de debate público se tienen que dotar de normas de funcionamiento y nombrar a un moderador o administrador que las aplique.
3. La UPCT puede habilitar, para uso de la comunidad universitaria, espacios para la prestación de servicios consistentes en la creación de recursos web institucionales o personales dentro de los dominios pertenecientes a la Universidad.
4. La creación de recursos web institucionales de carácter público la autoriza, de acuerdo con la Política de Seguridad de la UPCT, el Responsable de Información de la Universidad.
5. En la cesión de espacios web, la UPCT actúa de buena fe y no garantiza ni es responsable, directamente o subsidiariamente, de cualquier reclamación que se pueda derivar de su calidad, fiabilidad o exactitud, ni de los contenidos presentes a los sitios web a que eventualmente puedan conducir los hipervínculos incluidos en los recursos web.
6. Se desarrollará una normativa específica para regular la creación de espacios web dentro del dominio de la UPCT.

Artículo 10. Uso de servicios en la nube, no titularidad de la UPCT

1. La UPCT, a través de su Unidad de Informática y siempre que se cumplan los requisitos de seguridad necesarios, podrá contratar la prestación de servicios y/o uso de infraestructuras en la nube a un proveedor externo. A efectos de esta normativa, estos servicios e infraestructuras se considerarán “Sistemas de la UPCT” y se someterán al cumplimiento de su Política de Seguridad y de la presente normativa e instrucciones de desarrollo.
2. Los miembros de la UPCT que, para el desarrollo de sus tareas en el ámbito universitario, y con la autorización pertinente, usan servicios externos a los sistemas de la UPCT (nube), tienen la obligación de leer y comprender las condiciones legales de estos servicios, sabiendo en todo momento a qué se comprometen y qué responsabilidades tiene el prestador de servicios, y se tienen que asegurar que estas se ajustan al

ámbito normativo español. En cualquier caso, son los únicos responsables de su uso.

3. Excepto que el Comité de Seguridad TIC expresamente lo autorice, se prohíbe alojar información confidencial propia de la UPCT en servidores externos en “la nube” que no haya ofrecido la institución, en particular cuando se trate de datos de carácter personal contenidos en los sistemas de información en cuyo caso deberá someterse, adicionalmente, a la valoración del Delegado de Protección de Datos Personales.
4. Se prohíbe el uso de aplicaciones de computación en nube para tratar datos que estén bajo cláusula de confidencialidad o que contengan información sensible, de carácter estratégico para la institución o datos de terceras personas.
5. El usuario tiene que verificar que no hay cesión de ningún tipo de derecho de propiedad intelectual o industrial al proveedor del servicio.

Artículo 11. Medidas específicas

1. De forma específica se podrán articular dentro de este marco políticas, normas y recomendaciones de buen uso de servicios e infraestructuras concretas, que estarán disponibles en el espacio web de la UPCT, como pueden ser, entre otros:
   - Servicios telemáticos (correo electrónico, web, etc.).
   - Buen uso de la infraestructura de red y del acceso a Internet.
   - Teletrabajo seguro.
   - Administración segura de servidores.
   - Aulas de informática.
   - Contraseñas seguras.
   - Copias de seguridad.

TÍTULO III INCIDENTES DE SEGURIDAD: DETECCIÓN Y RESPUESTA

Artículo 12. Uso abusivo o indebido de los sistemas de información

1. En el uso de los recursos y servicios TIC de la UPCT los usuarios tienen que respetar los Estatutos de la Universidad, el ordenamiento jurídico y los derechos reconocidos en la Constitución española.
2. Además de lo antes indicado, se considera un mal uso o uso inaceptable a aquella actuación del usuario que puede afectar a la disponibilidad de un servicio, al trabajo del resto de usuarios, a la confidencialidad e integridad de la información o que, en general, ponga en riesgo cualquiera de las dimensiones de seguridad (disponibilidad, integridad,

confidencialidad, autenticidad y trazabilidad) de la información y los servicios.

3. La siguiente lista, aunque no es exhaustiva y no incluye todos los casos, constituye un conjunto de ejemplos de lo que se consideran malos usos:
    a) Incurrir en actividades ilícitas o ilegales de cualquier tipo, especialmente aquellas que puedan suponer perjuicio para los derechos, libertades e imagen de las personas.
    b) Uso de Internet para propósitos que puedan influir negativamente en la imagen de la UPCT, de sus representantes o de los organismos públicos o privados con los que se mantiene relación.
    c) El uso de una cuenta de usuario para la que no se tiene autorización o bien el robo de credenciales.
    d) El uso de la Red de la UPCT para conseguir el acceso no autorizado a cualquier ordenador, servidor o aplicación.
    e) Realizar de forma intencionada alguna actuación que interfiera en el funcionamiento normal de otros ordenadores, impresoras, dispositivos o redes.
    f) Instalar y ejecutar de forma intencionada en cualquier ordenador o subred cualquier tipo de software que provoque el mal funcionamiento o la sobrecarga en dicho equipo o subred (malware). También se incluye aquí la distribución de este malware a otros usuarios.
    g) El abuso deliberado de los recursos puestos a disposición del usuario.
    h) Los intentos de saltarse medidas de protección de la información o de explotar posibles fallos de seguridad de los sistemas.
    i) El no cumplimiento de las condiciones de las licencias del software o de sus derechos de autor.
    j) El envío de mensajes de correo de forma masiva (spam) o con contenido fraudulento, ofensivo, obsceno o amenazante.
    k) Ocultar o falsificar la identidad de una cuenta de usuario o de una máquina.
    l) El uso de los servicios de difusión de información para fines que no tengan relación con las propias del desempeño laboral o que no sean de interés para la comunidad universitaria.
    m) Los intentos de monitorización y rastreo de las comunicaciones de los usuarios.
    n) La lectura, copia, modificación o borrado de los ficheros de otros usuarios sin la autorización explícita del propietario.

4. Las acciones realizadas desde una cuenta de usuario o desde una cuenta de correo electrónico de usuario son responsabilidad de su titular.

5. Los sistemas se pueden configurar para prevenir acciones que puedan ser consideradas contrarias a esta normativa o a la Política de Seguridad de la UPCT. Estos sistemas pueden adoptar las medidas preventivas y de detección correspondientes.
6. Si algún Área o Departamento de la UPCT lleva a cabo actividades de docencia o investigación que requieran de un tratamiento especial en materia de seguridad, deberá ponerlo en conocimiento del Comité de Seguridad TIC o del Responsable de Seguridad.

Artículo 13. Incidentes de seguridad

1. Cuando un usuario detecte cualquier anomalía o incidencia de seguridad que pueda comprometer el buen uso y funcionamiento de los Sistemas de Información de la Universidad o su imagen, deberá informar inmediatamente a la Unidad de Informática (a través del Soporte a usuarios), que lo registrará debidamente y elevará, en su caso.
2. Delitos informáticos: La UPCT colaborará en la persecución de los delitos informáticos que tengan origen o destino en su infraestructura o usuarios, dando prioridad a los requerimientos que se reciban por parte de los órganos competentes y aportando toda la información que sea posible para el esclarecimiento del incidente; todo ello dentro del marco de la legalidad vigente.

Artículo 14. Monitorización y aplicación de esta normativa

Según su Política de Seguridad de la Información, la UPCT, por motivos legales, de seguridad y de calidad del servicio, y cumpliendo en todo momento los requisitos que al efecto establece la legislación vigente:

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 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.

La UPCT llevará a cabo esta actividad de monitorización de manera proporcional al riesgo, con las cautelas legales pertinentes y las señaladas en la jurisprudencia y con observancia de los derechos de los usuarios.
Los sistemas en los que se detecte un uso inadecuado o en los que no se cumplan los requisitos mínimos de seguridad, podrán ser bloqueados o suspendidos temporalmente. El servicio se restablecerá cuando la causa de su

inseguridad o degradación desaparezca. La Unidad de Informática, con la colaboración de las restantes unidades de la UPCT, velarán por el cumplimiento de la presente Normativa e informarán al Comité de Seguridad TIC sobre los incumplimientos o deficiencias de seguridad observados, al objeto de que se tomen las medidas oportunas.

El sistema que proporciona el servicio de correo electrónico podrá, de forma automatizada, rechazar, bloquear o eliminar parte del contenido de los mensajes enviados o recibidos en los que se detecte algún problema de seguridad o de incumplimiento de la presente Normativa.

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 o cualquier otro contenido inadecuado para las actividades desarrolladas por la UPCT. 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. El sistema permitirá el establecimiento de controles que posibiliten detectar y notificar a los administradores sobre usos prolongados e indebidos del servicio para que puedan tomarse las medidas correctoras y disciplinarias oportunas.

Artículo 15. Suspensión del uso de los recursos

1. La UPCT puede suspender, temporal o definitivamente, el uso de los recursos y servicios TIC a los usuarios, por razones:
    a. De operativa interna:
        - Cuando haya problemas en la disponibilidad de los recursos.
        - Cuando sea necesario para el mantenimiento y el correcto funcionamiento de los sistemas de la UPCT.
    b. De uso inadecuado de los recursos:
        - Cuando se hayan llevado a cabo actividades contrarias al ordenamiento jurídico.
        - Cuando se incumpla esta o cualquier otra normativa aprobada por la UPCT, que requiera la suspensión.
        - Cuando sea necesario para garantizar la seguridad de los recursos y sistemas.
    c. Por exigencia judicial. Cuando haya un requerimiento judicial que acuerde la adopción de la medida cautelar de suspensión del uso de los recursos y servicios TIC de la UPCT.

2. En los supuestos de suspensión en el uso de los recursos motivados por necesidades de operativa interna, la decisión se adoptará por el

Responsable del Sistema que lo comunicará con antelación a los usuarios.

3. Cuando la suspensión del uso de los recursos y servicios TIC, sea una medida preventiva a adoptar como consecuencia de un uso inadecuado de los mismos, el Comité de Seguridad será el órgano competente para acordar, de forma motivada, dicha suspensión. Una vez valorado el riesgo por parte de dicho Comité, se iniciaría de oficio el correspondiente procedimiento de suspensión de uso de los recursos TIC y se dará traslado al interesado de la presunta infracción para que realice las alegaciones que estime pertinentes en los plazos establecidos.

4. Cuando la suspensión del uso de los recursos y servicios TIC de la UPCT venga exigida por requerimiento judicial se dará traslado de este al Responsable del Sistema para que le dé cumplimiento.

5. La UPCT, mediante resolución rectoral, puede acordar la suspensión definitiva de la cuenta de usuario en los casos en que se constate un uso de los recursos TIC de la Universidad para actividades ilícitas o ilegales de cualquier tipo y, particularmente, para difundir contenidos o propaganda de carácter racista, xenófobo, pornográfico, sexista, de apología del terrorismo o atentatorio contra los derechos humanos, o actuar en perjuicio de los derechos a la intimidad, al honor, a la propia imagen o contra la dignidad de las personas. El Comité de Seguridad TIC deberá poner dichos hechos en conocimiento de las autoridades competentes por si los mismos pudieran ser constitutivos de infracción penal.

DISPOSICIÓN ADICIONAL PRIMERA

Esta Normativa de seguridad estará disponible en la web de UPCTlex (https://lex.upct.es/) y en el apartado de “Política de Seguridad y Normativa” dentro de la Sede Electrónica de la UPCT (https://sede.upct.es/).

DISPOSICIÓN ADICIONAL SEGUNDA

Periódicamente, el Comité de Seguridad TIC revisará la presente Normativa, que se someterá, de haber modificaciones, a la aprobación del Consejo de Gobierno de la UPCT, tal y como establece la Política de Seguridad de la Información de la UPCT.
La 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 o requeridos por incidentes de seguridad que puedan suceder.

DISPOSICIÓN ADICIONAL TERCERA.

Todos los artículos de esta normativa que emplean la forma del masculino genérico se entenderán aplicables a cualquier persona con independencia de su género.

DISPOSICIÓN DEROGATORIA

Esta *Normativa de Seguridad y uso de los recursos informáticos* deroga la aprobada el 7 de noviembre de 2011 por el Consejo de Gobierno.

DISPOSICIÓN FINAL

La presente normativa entrará en vigor al día siguiente de su publicación en el Tablón Oficial Electrónico de la Universidad.

GLOSARIO DE TÉRMINOS

- *Analizador de tráfico*: programa que monitoriza la información que circula por la red con el objeto de capturar información; se emplea a menudo el término inglés “sniffer”.
- *Autenticación*: Procedimiento para comprobar que alguien es quien dice ser cuando accede a un ordenador o a un servicio online.
- *Autenticidad*: La autenticidad en el envío de información a través de las redes es la capacidad de demostrar la identidad del emisor de esa información. El objetivo que se pretende es certificar que los datos, o la información, provienen realmente de la fuente que dice ser. Se puede utilizar también el término “no repudio”.
- *Comité de seguridad TIC*: Órgano colegiado que coordina las actividades de la universidad en materia de seguridad de la información.
- *Confidencialidad*: propiedad de la información, por la que se garantiza que está accesible únicamente a personal autorizado a acceder a dicha información. La confidencialidad de la información constituye la piedra angular de la seguridad de la in-formación. Junto con la integridad y la disponibilidad suponen las tres dimensiones de la seguridad de la información.
- *Credenciales*: Cada usuario se identifica en el sistema mediante una “cuenta de usuario”, que está compuesta por un identificador (único y distinto para cada usuario) y una o varias credenciales, asociadas a ese identificador y que sirven para verificar la identidad del usuario asociado a la cuenta (ver “Identificador”).
- *Dirección IP*: (del acrónimo inglés IP para Internet Protocol) es un número único e irrepetible con el cual se identifica a todo sistema conectado a una red. Así, una dirección IP (o simplemente IP) en su versión v4 es un conjunto de cuatro números del 0 al 255 separados por puntos. Por ejemplo: 192.168.121.40
- *Disponibilidad*: Se trata de la capacidad de un servicio o un sistema para ser accesible y utilizable por los usuarios o procesos autorizados cuando éstos lo requieran.
- *Herramienta de rastreo de puertos*: programa que monitoriza los servicios que ofrece un servidor conectado a una red; se usan por parte de los atacantes como forma de obtener información sobre posibilidades vulnerabilidades (puntos débiles) de un sistema.
- *Identificador*: Cada usuario se identifica en el sistema mediante una “cuenta de usuario”, que está compuesta por un identificador (único y distinto para cada usuario) y una o varias credenciales, asociadas a ese

identificador y que sirven para verificar la identidad del usuario asociado a la cuenta (ver “Credenciales”).

- *Incidente o incidencia de seguridad*: Cualquier suceso que afecte a la seguridad de los activos de información de la universidad, por ejemplo: acceso o intento de acceso a los sistemas; uso, divulgación, modificación o destrucción no autorizada de información, etc.
- *Integridad*: propiedad de la información, por la que se garantiza la exactitud de los datos transportados o almacenados, asegurando que no se ha producido su alteración, pérdida o destrucción, ya sea de forma accidental o intencionada, por errores de software o hardware o por condiciones medioambientales.
- *Monitorización*: Proceso para el registro y seguimiento de las acciones realizadas en un sistema o de la información tratada.
- *Principio de mínimos privilegios*: Principio según el cual los sujetos deben acceder exclusivamente a aquellos objetos que precisen inexcusablemente para ejecutar sus trabajos o procesos. Es término sinónimo de "necesidad de saber".
- *Política de Seguridad*: documento de nivel ejecutivo mediante el cual una Organización establece sus directrices de seguridad de la información.
- *Recurso TIC*: cualquier dispositivo, infraestructura, instalación, servicio o aplicación informática que dé cobertura al uso de las tecnologías de la información y las comunicaciones de apoyo a la gestión de los servicios y procedimientos y la información
- *Responsable del sistema*: Persona encargada de la explotación del sistema de información (ver la “Política de Seguridad de la Información de la UPCT” para más información sobre su identidad y responsabilidades).
- *Responsable de seguridad*: Persona encargada de velar por la seguridad de la información de la organización. El responsable de seguridad determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios (ver la “Política de Seguridad de la Información de la UPCT” para más información sobre su identidad y responsabilidades).
- *Trazabilidad*: Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad.
- *VPN (Red privada virtual)*: tecnología de red que permite una conexión virtual punto a punto entre dos equipos usando para la conexión una red pública como es Internet y consiguiendo que esta conexión sea segura gracias al cifrado de la comunicación. Una VPN es un caso práctico de aplicación de la Criptografía a las comunicaciones.