NORMATIVA DE SEGURIDAD Y USO DE LOS RECURSOS INFORMÁTICOS EN LA UPCT

El Consejo de Gobierno, en su sesión de 7 de noviembre de 2011, en virtud de lo dispuesto en el artículo 34 de los Estatutos, aprobó la presente normativa (modificada parcialmente en junio de 2015 y en sesión de Consejo de Gobierno de 12 de abril de 2016).

PREÁMBULO

La Política de Seguridad de la Universidad Politécnica de Cartagena (en adelante UPCT) se aprobó el 13 de abril de 2011 (https://sede.upct.es/politicadeseguridad.html); supone un marco general sobre el tratamiento de la seguridad de la información en el ámbito de nuestra universidad que debe ser desarrollado con normativas más específicas. Esta normativa desarrolla lo expuesto en la Política de Seguridad de la UPCT y aporta una serie de recomendaciones y obligaciones sobre el uso correcto de los sistemas de información, así como para desarrollar las buenas prácticas necesarias para la prevención, detección, respuesta y recuperación ante incidentes de seguridad.

El personal usuario de nuestra red y de nuestros sistemas de información deben respetar 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/as, no acaparar los recursos compartidos con el resto de usuarios/as y respetar las políticas de licencias de software. Esta normativa se debe aplicar a nuestra red, a todos los equipos conectados a ella y a toda la información contenida en estos equipos.

El/la responsable de Seguridad y los/las Responsables de los Sistemas deben ejercer las funciones y responsabilidades definidas en la Política de Seguridad de la UPCT.

No obstante, y con carácter general, se deben tener en cuenta los siguientes aspectos:

Quiénes deben conocer este documento:

- Los miembros de los Órganos de Gobierno, el personal directivo de los Departamentos y los/las responsables de los Servicios administrativos de la UPCT.
- Los miembros de la comunidad universitaria: profesorado, estudiantes, becarios/as de investigación, personal vinculado a proyectos de investigación, etc.
- El personal administrador de redes y sistemas, así como el resto del personal técnico.

- Cualquier otra persona o entidad externa que utilice los recursos informáticos de la Universidad o que preste servicios para la misma.

Esta Normativa de seguridad estará disponible en el apartado de "Política de Seguridad y Normativa" dentro de la Sede Electrónica de la UPCT (https://sede.upct.es/). Así mismo, podría encontrarse impresa en el Vicerrectorado de Tecnologías de la Información y las Comunicaciones y en la Unidad de Informática.

Por qué debe conocerse este documento:

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 u organismos que no se adecúen a las normas expuestas en este documento.

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

Lo expuesto en este documento se aplicará a todos los dispositivos conectados a nuestra red o con direccionamiento IP dentro del rango asignado a la UPCT, tales como PCs, portátiles, impresoras, dispositivos móviles, servidores. También se aplicará a aquellos dispositivos no pertenecientes a la UPCT pero que se conecten a la misma por distintas vías: red WiFi, VPN, servidores NAT, etc.

Políticas específicas y locales:

De forma específica se podrán articular dentro de este marco políticas y recomendaciones de buen uso de servicios e infraestructuras concretas, como pueden ser:

- Servicios telemáticos (correo electrónico, Web, etc.).
- Buen uso de la infraestructura de red y del acceso a Internet.
- Acceso a servidores con datos de carácter personal.
- Aulas de informática.
- Servidores departamentales.

Cuando sea necesario el uso de infraestructuras de red externas (como en nuestro caso lo es RedIris), las políticas y recomendaciones de uso de estas instituciones serán de aplicación en nuestra red.

Normas y recomendaciones de uso:

A continuación, y a modo de disposiciones generales, se plantean una serie de recomendaciones que pretenden regular el buen uso, disponibilidad y nivel de servicio de los recursos informáticos de la UPCT. Aquellas personas que de forma reiterada o

deliberada o por negligencia las ignoren o las infrinjan, se podrán ver sujetas a las actuaciones técnicas (para minimizar los efectos de la incidencia) o disciplinarias que se estimen oportunas.
En cualquier caso, será responsabilidad del Comité de Seguridad TIC el dar la difusión necesaria a esta normativa para que sea conocida por todos los agentes a los que se aplica.

Por otro lado, los cambios realizados en la modificación de 12 de abril de 2016 se realizan para alinear el documento con el Esquema Nacional de Seguridad (se han añadido los puntos g) e i) en el apartado 3 del Artículo 3, sobre las responsabilidades del personal usuario y recomendaciones mínimas).

ÍNDICE

DISPOSICIONES GENERALES

Artículo 1. Sobre la conexión y acceso a la Red de la UPCT y su gestión.

1. La Unidad de Informática es la responsable de la administración y gestión de la Red de la UPCT.

a) La instalación de nuevos puntos de red conectados a la Red de la UPCT se hará de conformidad con los criterios aprobados y será competencia exclusiva de la Unidad de Informática. Los trabajos correspondientes serán coordinados por 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 información y 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.

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 o de la responsable del equipo. No está permitida la conexión de equipos con nombres o direcciones no registrados. Si un equipo deja de usarse o se desconecta de la red, aunque sea sustituido por otro, se recomienda notificarlo a la Unidad de Informática para que se puedan registrar estos cambios en el DNS (servidor de nombres de dominio) o dar de baja la dirección IP para su posterior reutilización.

3. En el caso de los servidores departamentales, o sea, aquéllos instalados en un departamento y administrados por personal del mismo para dar un determinado servicio al personal adscrito al departamento, debe quedar claramente definida la persona que actúa como responsable del mismo y quién se encarga de su mantenimiento. Esta persona deberá responder ante incidencias e incumplimiento de esta Normativa por parte del sistema local. Este punto también será de aplicación para cualquier otro equipo de uso común (no asignado a un trabajador concreto) de los departamentos y unidades.

4. Para poder proporcionar acceso a terceros mediante la red inalámbrica de la UPCT se requerirá la autorización correspondiente. Existe un formulario para la solicitud de alta temporal de personal usuario externo en nuestra red inalámbrica.

5. 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.

Artículo 2. Sobre el buen uso de la Red.

1. El personal usuario de la red no debe utilizar esta infraestructura y servicios para otros usos que no sean los permitidos en la Política de uso de RedIRIS (http://www.rediris.es/rediris/instituciones/politica_de_uso.pdf) o los propios necesarios para el desempeño de su actividad.

2. En aquellos casos en que la actividad docente o investigadora, para realizar determinadas pruebas, así lo requiera (por el fuerte impacto que pudiera tener en el entorno de "producción"), éstas se realizarán en un entorno diferenciado del de producción.

3. Se deben emplear mecanismos seguros (protocolos seguros, VPNs) para conexiones externas a nuestra red que requieran de unas condiciones de confidencialidad, integridad y autenticidad altas.

4. Ningún usuario/a 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 y bajo situaciones especiales (incidentes de seguridad, denuncias de usuarios/as, etc.) que lo justifiquen.

Artículo 3. Sobre las responsabilidades del personal usuario y recomendaciones mínimas (1).

1. La responsabilidad del uso adecuado de las herramientas informáticas, como el ordenador personal, los periféricos y sus programas instalados, así como de las cuentas para el acceso a los servicios y aplicaciones, es del propio personal usuario. El usuario/a de equipos personales debe procurarse los conocimientos imprescindibles para el manejo de sus programas, así como realizar copias de seguridad de los datos que considere relevantes; para ello se recomienda utilizar los servicios que pone a su disposición la Universidad.

2. La intervención de personal técnico de la Unidad de Informática en un puesto de trabajo requerirá la presencia del responsable del equipo o de la persona en quien éste delegue.

3. En cualquier caso, a continuación se plantean unas recomendaciones sobre los aspectos mínimos de seguridad que deben ser tenidos en cuenta por todo el personal usuario:

(1) Se añaden los puntos g) e i) al apartado 3 (Consejo de Gobierno de 12 de abril de 2016).

a) **Actualizaciones del Sistema Operativo**: Los equipos conectados a nuestra red deben estar al día en cuanto a las actualizaciones del Sistema Operativo; para ello el usuario/a debe conocer el mecanismo para la descarga de los parches de actualización de su sistema operativo y realizar dichas actualizaciones siempre que sean consideradas por el fabricante como “críticas” o “importantes”. Como buena práctica se recomienda revisar la existencia de parches al menos una vez cada 15 días. La única excepción será para los casos de no compatibilidad con aplicaciones necesarias para el trabajo del personal usuario.

b) **Antivirus**: Todos los equipos deben tener activo y actualizado un software antivirus; la UPCT dispone de una licencia corporativa de Software antivirus gestionada por la Unidad de Informática.

c) **Cortafuegos personales**: Es recomendable que todos los dispositivos móviles que se conecten a nuestra red tengan activo un cortafuegos personal, basado en un software instalado en la propia máquina y debidamente configurado.

d) **Contraseñas**:

- El acceso a los distintos servicios de red y ordenadores se hará mediante las correspondientes credenciales, con los privilegios adecuados y cumpliendo los mínimos establecidos en la Política de contraseñas.
- La UPCT dispone de un repositorio de usuarios/as y contraseñas (directorio LDAP) y se recomienda que todos los procesos de autenticación para uso de los servicios telemáticos (incluidos los departamentales) se realicen contra este directorio; la Unidad de Informática dará la información necesaria al personal administrador de los servicios para que puedan implementar este proceso de autenticación.
- La comunicación para el envío de las credenciales del personal usuario debe ser siempre encriptada, según los estándares mínimos que se establezcan en la Política de contraseñas.
- La Unidad de Informática nunca solicitará al personal usuario sus credenciales (usuario/contraseña) por correo electrónico o cualquier otro medio inseguro. Especialmente, insistir en que estas credenciales no deberán proporcionarse por parte del personal usuario bajo ningún requerimiento, salvo los medios debidamente habilitados (Portal de Servicios) para su mantenimiento.
- Se fomentará el uso de **certificados electrónicos y DNI electrónico** como medios seguros de autenticación. El personal usuario también será responsable del uso de los certificados electrónicos que se le proporcionen; en caso de que se produzca alguna incidencia (pérdida, robo, etc.) de un certificado electrónico expedido a través de los puntos de registro de la UPCT, el personal usuario deberá contactar con la Unidad de Informática para su revocación o anulación.

e) **Protección física del equipo (protección de escritorio y acceso local)**: 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 personal usuario para reanudar la actividad en curso. Asimismo se limitará el número de accesos fallidos y se registrarán todos los accesos (con éxito o no) y se informará al personal usuario del último acceso con su identidad con éxito.

f) **Servicios o aplicaciones no necesarias**: Si una aplicación no es necesaria para el trabajo del personal usuario del equipo, no debe estar instalada y el personal técnico de la Unidad de Informática puede requerir al usuario/a la desinstalación de la misma.

g) El **acceso remoto** (desde Internet) a ordenadores y servidores conectados a la red de la UPCT se hará exclusivamente utilizando mecanismos seguros de conexión.

h) El uso del **software instalado** en equipos informáticos de la Universidad debe ajustarse a la normativa legal vigente. En consecuencia, el personal usuario debe 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 personal usuario.

i) El personal usuario deberá informar a la Unidad de Informática de cualquier incidente que pueda afectar a la seguridad de la información o de su equipo.

j) Las medidas enumeradas en los apartados anteriores a), b) d), e), f), g) e i) serán de obligado cumplimiento para aquellos equipos y servicios que manejen información propia de los sistemas catalogados dentro del Esquema Nacional de Seguridad (ENS) en la UPCT.

Artículo 4. Sobre lo que no está permitido: el mal uso de las infraestructuras y servicios.

1. Se considera un mal uso o uso inaceptable a aquella actuación del personal usuario que puede afectar a la disponibilidad de un servicio, al trabajo del resto de usuarios/as, a la confidencialidad y seguridad de la información o que, en general, ponga en riesgo cualquiera de las cinco dimensiones de seguridad (disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad) de la información y los servicios.

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:

- El uso de una cuenta de usuario/a para la que no se tiene autorización o bien el robo de credenciales (usuario/a y contraseña).
- El uso de la Red de la UPCT para conseguir el acceso no autorizado a cualquier ordenador, servidor o aplicación.
- Realizar alguna actuación de forma intencionada que interfiera en el funcionamiento normal de otros ordenadores, impresoras, dispositivos o redes.

- 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 cesión de este malware a otras personas usuarias.
- El abuso deliberado de los recursos puestos a disposición del personal usuario.
- Los intentos de saltarse medidas de protección de la información o de explotar posibles fallos de seguridad de los sistemas.
- El no cumplimiento de las condiciones de las licencias del software o de sus derechos de autor/a.
- El envío de mensajes de correo con contenido fraudulento, ofensivo, obsceno o amenazante.
- Ocultar o falsificar la identidad de una cuenta de usuario/a o de una máquina.
- 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.
- Los intentos de monitorización y rastreo de las comunicaciones de los/las usuarios/as.
- La lectura, copia, modificación o borrado de los ficheros de otras personas usuarias sin la autorización explícita del propietario/a.

2. Las anteriores actividades no se considerarán de “mal uso” cuando estén debidamente aprobadas por el/la Responsable de los Servicios TIC o por el Comité de Seguridad.

Artículo 5. Las consecuencias del mal uso de los recursos.

1. Colaboración del personal usuario. El personal usuario, cuando se le solicite, debe colaborar con el personal administrador de sistemas, en la medida de sus posibilidades, en cualquier investigación que se haga sobre mal uso de los recursos, aportando la información que se les requiera.

2. Acciones correctivas y preventivas. Si el personal administrador del sistema detecta la existencia de un mal uso de los recursos y éste procede de las actividades o equipo de un usuario/a determinado, puede tomar cualquiera de las siguientes medidas para proteger a las otras personas usuarias, redes o equipos:

- Notificar la incidencia al personal usuario o responsable del sistema.
- Suspender o restringir el acceso o uso de los servicios mientras dure la investigación. Esta suspensión podrá ser recurrida por el personal usuario ante la autoridad competente.
- Con el permiso del responsable de seguridad y la debida justificación, inspeccionar ficheros o dispositivos de almacenamiento del personal usuario implicado.
- Informar al Comité de Seguridad u órganos de gobierno correspondientes de lo sucedido.

3. Estudiantes. Las incidencias relativas a alumnado se tratarán en colaboración con el Vicerrectorado de Estudiantes y Extensión Universitaria.

4. Medidas disciplinarias. En caso que fuera necesario, corresponderá al órgano de gobierno competente la adopción de medidas disciplinarias hacia el personal usuario infractores de esta política, una vez informado por el Comité de Seguridad TIC y por el/la Responsable de la Información.

5. Delitos informáticos. La UPCT colaborará en la persecución de los delitos informáticos que tengan origen o destino en su infraestructura o usuarios/as, 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.

DISPOSICIÓN FINAL (2)

La presenta Normativa entrará en vigor al día siguiente de su publicación en el Tablón Oficial Electrónico de la UPCT.

(2) Se añade la Disposición Final (Consejo de Gobierno de 12 de abril de 2016).