Normativa de seguridad y uso de los recursos informáticos en la UPCT

Aprobada por: Consejo de Gobierno de la UPCT.

Fecha:

Resumen:

La Política de Seguridad de la 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.

Los usuarios 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, no acaparar los recursos compartidos con el resto de usuarios 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 responsable de Seguridad y los Responsables de los Sistemas deben ejercer las funciones y responsabilidades definidas en la Política de Seguridad de la UPCT.

Quiénes deben conocer este documento:

- Los miembros de los Órganos de Gobierno, los Directores de los Departamentos y los responsables de los Servicios administrativos de la UPCT.
- Los miembros de la comunidad universitaria: profesorado, estudiantes, becarios de investigación, personal vinculado a proyectos de investigación, etc.
- Los administradores 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 Nuevas Tecnologías y en la Unidad de Informática.

Por qué debe conocerse este documento:

La Universidad Politécnica de Cartagena 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 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.

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

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

- 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 y la Unidad Técnica.
- 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.
- Los equipos electrónicos de gestión e infraestructura de la red de la UPCT serán instalados, configurados y mantenidos exclusivamente por la Unidad de Informática.
- 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.

1.2. 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 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.

1.3. 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 la política 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.

1.4. 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 un usuario externo en nuestra red inalámbrica.

1.5. 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.

2. Sobre el buen uso de la Red:

2.1. 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 (http://www.rediris.es/rediris/instituciones/politica_de_uso.pdf) o los propios necesarios para el desempeño de su actividad.

2.2. 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"), estas se realizarán en un entorno diferenciado del de producción.

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

2.4. 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 y bajo situaciones especiales (incidentes de seguridad, denuncias de usuarios, etc.) que lo justifiquen.

3. Sobre las responsabilidades de los usuarios y recomendaciones mínimas.

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 usuario. El usuario 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.

La intervención de un 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.

En cualquier caso, a continuación se plantean unas recomendaciones sobre los aspectos mínimos de seguridad que deben ser tenidos en cuenta por todos los usuarios:

3.1. **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 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 usuario.

3.2. **Antivirus**: Todos los equipos deben tener activo y actualizado un software antivirus; se recomienda usar el software antivirus corporativo, licenciado por la Unidad de Informática.

3.3. **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.

3.4. **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 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 a los administradores de los servicios para que puedan implementar este proceso de autenticación.
- La comunicación para el envío de las credenciales del usuario debe ser siempre encriptada, según los estándares mínimos que se establezcan en la Política de contraseñas.
- La Unidad de Informática nunca solicitará al usuario sus credenciales (usuario/contraseña) por correo electrónico o cualquier otro medio inseguro. Especialmente insistimos en que estas credenciales no deberán proporcionarse por parte del 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 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 usuario deberá contactar con la Unidad de Informática para su revocación o anulación.

3.5. **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 usuario para reanudar la actividad en curso. Así mismo se limitará el número de accesos fallidos y se registrarán todos los accesos (con éxito o no) y se informará al usuario del último acceso con su identidad con éxito.

3.6. **Servicios o aplicaciones no necesarias**: Si una aplicación no es necesaria para el trabajo del usuario del equipo, no debe estar instalada y el personal técnico de la Unidad de Informática puede requerir al usuario la desinstalación de la misma. Tampoco se debe instalar software que permita el acceso remoto al equipo de forma no autenticada.

3.7. 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.

3.8. Las medidas 3.1, 3.2, 3.4, 3.5 y 3.6 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.

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

4.1. 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 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 para la que no se tiene autorización o bien el robo de credenciales (usuario 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 otros usuarios.
- El abuso deliberado de los recursos puestos a disposición del 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.
- El envío de mensajes de correo con contenido fraudulento, ofensivo, obsceno o amenazante.
- Ocultar o falsificar la identidad de una cuenta de usuario 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 usuarios.
- La lectura, copia, modificación o borrado de los ficheros de otros usuarios sin la autorización explícita del propietario.

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

5. Las consecuencias del mal uso de los recursos:

5.1. **Colaboración de los usuarios:** Los usuarios, cuando se les solicite, deben colaborar con los administradores 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.

5.2. **Acciones correctivas y preventivas:** Si los administradores del sistema detectan la existencia de un mal uso de los recursos y éste procede de las actividades o equipo de un usuario determinado, pueden tomar cualquiera de las siguientes medidas para proteger a los otros usuarios, redes o equipos:

- Notificar la incidencia al 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 usuario ante la autoridad competente.

- Con el permiso del responsable de seguridad y la debida justificación, inspeccionar ficheros o dispositivos de almacenamiento del usuario implicado.
- Informar al Comité de Seguridad u órganos de gobierno correspondientes de lo sucedido.

5.3. **Estudiantes:** Las incidencias relativas a alumnos se tratarán en colaboración con el Vicerrectorado de Estudiantes.

5.4. **Medidas disciplinarias**: En caso que fuera necesario, corresponderá al Órgano de gobierno competente la adopción de medidas disciplinarias hacia los usuarios infractores de esta política, una vez informado por el Comité de Seguridad TIC y por el Responsable de la Información.

5.5. **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.