NORMATIVA DE USO DE LABORATORIOS Y AULAS INFORMATIZADAS

(Extraído del Texto Refundido de las Normativas vigentes en el Ámbito de las TIC aprobado por el acuerdo del Consell de Govern en fecha de 11 de julio de 2011)

Título IV. Medidas de seguridad para las personas usuarias de los recursos tecnológicos de la UAB

Capítulo I. Disposiciones generales

Artículo 40. Derecho de uso de los sistemas informáticos de la UAB

Los recursos informáticos de la Universitat Autònoma de Barcelona, tanto los de las instalaciones centrales como los del resto de las instalaciones distribuidas, incluyendo sistemas centrales/distribuidos, estaciones de trabajo, ordenadores personales, redes internas y externas, software, sistemas multiusuarios, etc. son para uso exclusivo de las tareas propias de la Universidad por parte de los miembros de su comunidad o personas autorizadas.

Artículo 41. Ámbito de aplicación

1. Dado que la mayoría de los sistemas informáticos de la Universidad están conectados directa o indirectamente con la red general de la Universidad, y que el mal uso o la falta de sistemas de seguridad adecuados en uno de estos sistemas pueden comprometer la seguridad de los otros sistemas de la Universidad o de las instituciones a las cuales la red general de la Universidad está conectada, el contenido de este título se aplica a todo aquél que haga uso de los sistemas informáticos de la Universidad o que disponga de sistemas o redes conectadas directa o indirectamente con la red general.

2. Las personas que soliciten o dispongan de acceso a los sistemas informáticos (ya sean propios o de la UAB) o de una conexión de su sistema o de su red a la red general de la Universidad deberán conocer las medidas de seguridad de los recursos informáticos, los cuales estarán a su disposición a través del portal de la UAB.

3. La Universidad se reserva el derecho de iniciar las acciones legales oportunas cuando se vean vulnerados sus derechos como consecuencia del uso inadecuado de sus recursos informáticos, y de poner a disposición de las autoridades competentes toda la información disponible en caso de denuncias por mal uso y vulneración de derechos de terceros.

Capítulo II. De los sistemas informáticos

Artículo 42. Asignación de recursos de los sistemas informáticos

Para la asignación de recursos de los sistemas informáticos (institucionales, centrales o departamentales), y para la conexión de sistemas y de redes a la red general se reconoce un responsable de los recursos informáticos y de dos categorías de usuarios/as: administrador/a de recursos informáticos y usuario/a final.

Artículo 43. Responsable de los recursos informáticos

1. La persona responsable de los recursos informáticos es la persona que ha de velar por el buen funcionamiento de los recursos informáticos que tiene asignados bajo su tutela siempre con el soporte de los servicios centrales y distribuidos.

2. Son responsables de los recursos informáticos:

a) Los/as decanos/as y los/as directores/as de centro son responsables de los recursos de uso general para la docencia del centro.
b) Los/as directores/as de departamento son responsables de los recursos informáticos de los laboratorios de prácticas, de los destinados a la investigación y de los servicios informáticos de gestión del departamento.
c) Los/as administradores/as de centro son responsables de los recursos destinados a la gestión del centro.
d) Los/as directores/as de los servicios y de los institutos son responsables de todos los recursos que utilicen.
e) El/la director/a de TIC es responsable de los recursos centrales y de la red de comunicaciones con el apoyo de los jefes de los servicios de informática distribuida en el caso de los centros de la UAB.

3. La persona responsable de los recursos informáticos podrá delegar las funciones, pero no la responsabilidad, que crea que son necesarias para controlar el uso de los recursos informáticos.

Artículo 44. El/la administrador/a de los recursos informáticos

1. El/la administrador/a de los recursos informáticos es la persona encargada de gestionar uno o más recursos informáticos (sistemas multiusuario, estaciones de trabajo, ordenadores personales, redes internas, etc.) conectados directa o indirectamente a la red general de la Universidad.

2. El/la administrador/a de los recursos informáticos trabajará de manera coordinada con la persona responsable los recursos informáticos y los servicios, a la cual comunicará todas las incidencias que haya detectado y que puedan afectar el buen funcionamiento de los recursos.

3. El/la administrador/a de los recursos informáticos tendrá que aplicar el contenido de este título a los recursos que gestiona i a los/as usuarios/as que dependen d él/ella. Igualmente deberá aplicar las otras normativas específicas que existan.

4. El/la administrador/a de los recursos informáticos se compromete a trabajar de manera coordinada con los servicios centrales en todas las cuestiones vinculadas a la prestación del servicio pero sobre todo en cuestiones técnicas y de seguridad, y a colaborar activamente en la detección, el seguimiento y la identificación de las posibles personas implicadas en la vulneración del contenido de este título.

Artículo 45. El/la usuario/a final

1. El/la usuario/a final es la persona que usa un recurso informático (propio, cedido por la UAB o de propiedad de la UAB) que esté conectado directa o indirectamente con la red general de la Universidad.

2. El/la usuario/a final se compromete a seguir las recomendaciones en cuanto al uso de los recursos informáticos establecidas por la UAB, y las de las personas responsables y administradores de los recursos informáticos especialmente en cuestiones técnicas, de protección de datos de carácter personal, de material con derechos de autor y en cuestiones de seguridad (básicamente respecto al uso de la red, la actualización de los programas antivirus y las políticas de acceso y custodia de la información).

3. El/la usuario/a está obligado/a a comunicar a las personas responsables pertinentes cualquier cambio en la titularidad de los recursos informáticos que tenga asignados y, mientras esta comunicación no se produzca, continúa siendo la única persona responsable a todos los efectos de los usos que se deriven.

4. La persona responsable de los recursos informáticos, por motivos de incumplimiento de la presente normativa, podrá denegar, de manera preventiva y provisional, el uso o acceso a un sistema informático, o la conexión de un sistema o red a la red general de la Universidad. En caso de desconexión de la red, previamente se contactará con la persona responsable

para comunicarle la acción pertinente y solucionar los problemas (excepto que se vea comprometida la seguridad de la red –o de segmentos de la red– y que sea imperativa su desconexión).

Capítulo III. Responsabilidades de las personas usuarias

Artículo 46. Protección de datos, palabras clave y uso de recursos

1. Las personas usuarias tendrán máximo cuidado en la manipulación y uso de los equipos informáticos, y de toda la infraestructura complementaria. Evitarán llevar a cabo cualquier acción, que de manera voluntaria o involuntaria, pueda perjudicar la integridad física de la maquinaria o de la instalación (destrozo, sustracción, traslado no autorizado, etc.) o la integridad lógica del software o los datos.

2. Las personas usuarias accederán a los recursos informáticos siguiendo las normativas específicas de cada centro, y accederán a los sistemas informáticos siguiendo las recomendaciones particulares que los servicios informáticos y las personas responsables de recursos hayan estipulado.

3. Los recursos informáticos de la Universidad son un bien público y su finalidad es almacenar, servir y tratar información vinculada a las actividades de la Universidad. Por razones de seguridad, el/la administrador/a de los recursos informáticos podrá inspeccionar, de manera ordinaria, la información contenida en los sistemas informáticos que administre. En caso que, por razones de seguridad, haya que hacer una inspección más específica, el/la administrador/a de los recursos informáticos deberá justificarlo a la persona responsable de los recursos informáticos.

4. Las cuentas de usuario en los sistemas informáticos de la Universidad son personales e intransferibles.

5. Es responsabilidad de la persona usuaria tener el máximo cuidado de su palabra clave, para lo cual, sobretodo, la mantendrá secreta, usará palabras claves que no sean triviales, la cambiará periódicamente y siempre que crea o sospeche que su confidencialidad puede ser violada.

6. Todos los cambios de palabras clave de cuentas de los sistemas informáticos se llevarán a cabo utilizando los mecanismos y protocolos definidos en cada momento por las personas responsables de los sistemas.

7. La persona usuaria se compromete a no utilizar los recursos públicos (ordenadores, red, puntos de conexión, etc.) para realizar actividades que no estén vinculadas estrictamente con la actividad académica o de investigación y será responsabilidad suya todo el material almacenado o descargado con derechos de autor y que no disponga de la licencia correspondiente. Además, la persona usuaria se compromete a respetar los términos indicados en la Ley orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal y la UAB podrá tomar las decisiones oportunas en relación con las acciones que se deriven de estos hechos.

Artículo 47. Incumplimiento de la normativa

1. Se considera incumplimiento de las condiciones de uso de los recursos informáticos en lso siguientes supuestos:

a) El uso ilícito por parte de terceras personas de las cuentas de usuario en los sistemas informáticos (con conocimiento o no de las personas usuarias legítimas), tanto en respecto a la persona que lleva a cabo el acceso indebido como a la persona responsable de la cuenta.

b) La desprotección de la información de las personas usuarias de manera que faciliten un acceso parcial o generalizado.

c) El uso indebido de los servicios de red y de los medios electrónicos para comunicarse con otras personas usuarias de los sistemas informáticos, de la red de la Universidad o de las redes a las cuales la Universidad está conectada, cuando ocasionen molestias (mensajes molestos u ofensivos, acoso electrónico, suplantación de direcciones de red, etc.), o bien no se respete el contenido de este título o las normativas de las instituciones y las redes con las cuales y mediante las cuales se comuniquen. También se considerará incumplimiento el acceso a paquetes de comunicación para averiguar información de la cual no se es propietario.

d) La búsqueda de palabras clave de otras personas usuarias o cualquier intento de encontrar y explotar agujeros en la seguridad de los sistemas informáticos de la Universidad o de fuera, o hacer uso de esos sistemas para atacar cualquier sistema informático.

e) La creación, el uso o el almacenamiento de programas o de información que puedan ser utilizados para atacar los sistemas informáticos de la Universidad o de fuera.

f) El destrozo, la sustracción o el traslado no debidamente autorizado a otras dependencias, de cualquier elemento físico de la instalación informática o de infraestructura complementaria.

g) La alteración de la integridad de los datos.

h) Cualquier otra actuación que vulnere la normativa vigente o que afecte o menostenga las condiciones de uso de los recursos informáticos.

Artículo 48. Medidas aplicables

1. El incumplimiento del contenido de este título en cualquier grado comportará la suspensión del acceso a los sistemas informáticos, y/o la desconexión de los sistemas o redes a la red general de la Universidad.

2. En los casos de incumplimiento de la normativa, las personas responsables de los recursos informáticos, previa audiencia de la persona interesada, podrán aplicar preventivamente la medida prevista en este artículo, si bien esta medida deberá ser confirmada por la Comisión de Disciplina Informática. A la vista de los hechos y las circunstancias que concurran, esta comisión establecerá la duración y, si es necesario, la periodicidad necesaria para confirmar la medida.

3. Contra las resoluciones de este órgano, las personas interesadas podrán interponer recurso ordinario ante el/la rector/a o la persona en la cual delegue.

4. La persona responsable de los recursos informáticos podrá elevar a la Comisión de Disciplina Informática aquellos casos que, sin estar explícitamente contemplados en el presente título, pueda considerar sancionables.

5. Las medidas mencionadas en este artículo se aplicarán sin perjuicio de las acciones disciplinarias, civiles o penales que sea necesario aplicar a las personas presuntamente implicadas, así como de la reparación de los daños ocasionados.

Capítulo IV. Grupo de Trabajo para la Coordinación de Incidentes en Sistemas Informáticos (CSIRT-UAB)

Artículo 49. Objetivos y funciones

El objetivo de este grupo es trabajar y asesorar en temas de seguridad informática y gestión de incidentes en las redes telemáticas de la UAB. Este grupo tendrá como objetivos principales:

a) Coordinar las políticas de trabajo sobre vulnerabilidades de seguridad y amenazas.
b) Definir las líneas de trabajo para divulgar y poner a disposición de la comunidad información que permita prevenir y resolver incidentes de seguridad.
c) Formular las políticas de difusión y educación de la comunidad en el ámbito de la seguridad informática.
d) Definir las reglas de actuación per llevar a cabo investigaciones (proactivas) relacionadas con la seguridad informática

Disposición final

Este texto refundido entrará en vigor al día siguiente de su aprobación por el Consell de Govern.

Anexo II: Guía de buenas prácticas en la comunicación electrónica de la UAB

1. Recomendaciones de carácter general

a) Mantener al día les actualizaciones del software y del sistema operativo, especialmente el antivirus, y, en la medida que sea posible, usar el software recomendado. (Consultad el apartado "Maquinari i programari recomanat" en http://www.uab.cat/si.)

b) Controlar periódicamente el buzón de correo (cuya capacidad es limitada), para evitar que se quede sin espacio libre (por ejemplo, traspasar los correos que se quieran conservar a carpetas locales y hacer copias de seguridad de éstas; se hacen copias del buzón institucional automáticamente). Las personas que os envíen correos agradecerán que no tengáis el buzón lleno (no les llegará un mensaje de rechazo) y también os lo agradecerá el servidor de correo.

c) Descargar los ficheros adjuntos que sean útiles (sin imprimir el contenido del mensaje si no es realmente necesario, ya que el coste del espacio en disco es más de 150.000 veces inferior que el coste de impresión) y eliminar el mensaje (o también moverlo a una carpeta local). Acordarse de vaciar la papelera y la carpeta de correos enviados siempre que sea posible.

d) Proteger las palabras clave de acceso a los buzones de correo electrónico y evitar la divulgación a terceras personas. En caso de pérdida o de desconfianza que alguien las pueda usar, cambiarlas tan pronto como sea posible a través de la página http://sia.uab.es/gestio_pwd.html.

NORMATIVA DE FUNCIONAMIENTO PROPIA DEL SID DE LAS FACULTADES DE CIENCIAS Y BIOCIENCIAS

1.- El Servicio de Informática Distribuida de las Facultades de Ciencias y Biociencias tiene como función fundamental dar apoyo a la docencia de las titulaciones que se imparten en las facultades. La responsabilidad de su gestión recae en los respectivos decanatos.

2.- La correcta configuración y adecuación de los medios específicos necesarios para la docencia de una asignatura son responsabilidad del profesor encargado de impartirla. Por este motivo, el profesor colaborará en la instalación y configuración de los medios mencionados, asegurándose de su correcto funcionamiento. Los técnicos del SID proporcionarán el soporte técnico oportuno.

3.- El software que se proporcione para su instalación deberá disponer de las correspondientes licencias de uso. Aquel software que no se haya proporcionado teniendo en cuenta el protocolo establecido a tal efecto, o que no sea comprobado su correcto funcionamiento, no podrá tener garantizada su disponibilidad ni su correcta funcionalidad.

4.- En todas aquellas actividades que requieran la presencia de un profesor, este podrá solicitar la reserva de un espacio del SID, para uso exclusivo. Las reservas se dirigirán al coordinador de la titulación correspondiente, el cual las tramitará al SID de forma conjunta. Deberá procurarse que las reservas de una asignatura no se concentren en períodos cortos de tiempo, sino que se repartan a lo largo del período lectivo.

5.- El SID enviará, con suficiente antelación, una circular de aviso de apertura del período de solicitudes de reserva a los coordinadores de titulación; será la responsabilidad de los coordinadores hacer extensiva la información de las circulares a todos los profesores de su titulación. Puntualmente también se podrán solicitar reservas de espacios dirigiéndose directamente al SID con una antelación mínima de 15 días.

6.- El coordinador del SID adecuará los grupos de prácticas a los espacios más adecuados del SID en función de las distintas capacidades de ésta, con el objetivo de optimizar los recursos. A partir de la información recibida, el coordinador del SID planificará los horarios de los períodos docentes, tratando de respetar los horarios de reserva propuestos y resolviendo los posibles conflictos entre titulaciones, con tal de garantizar el uso racional de los recursos y su provecho.

7.- Los estudiantes de las facultades podrán solicitar, mediante reserva, el uso libre (sin presencia de profesor) de los ordenadores de las aulas informatizadas, sin perjuicio de la prioridad de uso para la docencia.

8.- Para el uso libre de los ordenadores, la reserva se hará en un período no superior a las dos horas diarias, y, con la antelación que determine la web de reservas habilitada a tal efecto.

9.- El uso de los ordenadores de las aulas informatizadas está destinado fundamentalmente al ámbito docente. No está permitido el uso de aplicaciones ajenas a este ámbito ni, en general, todo aquel software que no haya sido instalado por el personal técnico del SID. Todos los casos especiales que hagan necesarias otras configuraciones deberán ser comunicados a los responsables del SID y debidamente autorizados.

10.- Cualquier recurso específico que se requiera deberá ser solicitado al personal técnico del SID. No se permite sacar de los espacios físicos del SID ningún tipo de recurso, físico o lógico, ni modificar su configuración sin una autorización expresa. Así mismo, está prohibida la suplantación de direcciones IP y la extracción no autorizada de información procedente de

la red. Tampoco se podrá modificar o eliminar el sistema de particiones que esté establecido en los PCs.

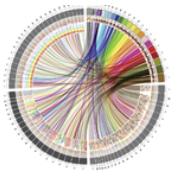
11.- Está prohibido expresamente comer o beber en las aulas informatizadas, así como hacer uso lúdico de los ordenadores. Se deben mantener los espacios limpios. Se ruega cuidar los recursos i respetar el trabajo de los otros usuarios.

12.- Los usuarios del SID podrán enviar las quejas o sugerencias que consideren oportunas mediante un email desde la propia página web del SID o desde un *applet* instalado en cada ordenador de las aulas informatizadas.

Universitat Autònoma de Barcelona

UAB CEI CAMPUS D'EXCEL·LÈNCIA INTERNACIONAL

MSc in Bioinformatics



Yo, ...

he **leído** y **acepto** el cumplimiento de la **Normativa de uso de laboratorios y aulas informatizadas** y la **Normativa de funcionamiento propia del SID de las Facultades de Ciencias y Biociencias**.

Para que así conste, firmo el presente papel a fecha ..... de ..... de 20....