UNIVERSIDAD
ALFONSO X EL SABIO

REGLAMENTO DE USO DE LOS RECURSOS INFORMATICOS Y DE COMUNICACIONES

EXPOSICIÓN DE MOTIVOS

El protagonismo que han adquirido las nuevas tecnologías, medios de comunicación y telecomunicaciones en general, se ha trasladado a las sociedades de todo el mundo y, en pleno sigo XXI, no sería posible un desarrollo social y económico que trabajase al margen de las propias tecnologías de la información.

No en vano, el manejo y dominio de los instrumentos informáticos se ha convertido en la base técnica imprescindible para la adecuada adaptación de la actividad empresarial al dinamismo tecnológico de la sociedad. La complejidad de los medios informáticos y de comunicaciones exige una regulación apta para conseguir un uso racional del material técnico, que proteja la calidad de los aparatos e instalaciones y permita la docencia y la investigación a través de unos recursos limitados, redundando en beneficio de la comunidad universitaria.

La generalización del acceso a la red Internet y su integración en los hábitos culturales y sociales ha creado un nuevo espacio de comunicación y convivencia que enriquece y estimula el afán de conocimiento, la creatividad y la sociabilidad, pero que se presta a la aparición de los mismos conflictos que cualquier otro entorno social.

La mayoría de los sistemas informáticos de la Universidad están conectados directa o indirectamente a la Red general de la Universidad. Por tanto, el mal uso o la ausencia 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 que la red de la Universidad está conectada.

Por ello, se requiere un marco normativo adecuado, que facilite el acceso a dichos recursos, que proteja la intimidad de las personas y que asegure la máxima eficiencia de dichos recursos compartidos.

Título I
Disposiciones Generales

Artículo 1.- Objeto

1. El propósito de esta Normativa de uso de los Recursos Informáticos y de Comunicaciones (en adelante, RIC) de la Universidad Alfonso X el Sabio es asegurar que dichos recursos se utilizan con los fines de Docencia, Investigación y Servicios Administrativos, propios de aquélla. Así mismo, se pretende conseguir los siguientes objetivos:

   a) Proteger el prestigio y el buen nombre de la Universidad Alfonso X el Sabio así como el de las personas e instituciones asociadas.

   b) Garantizar la seguridad, rendimiento y privacidad de los sistemas y máquinas, tanto de la Universidad Alfonso X el Sabio como de terceros.

   c) Evitar situaciones que puedan causar a la Universidad Alfonso X el Sabio algún tipo de responsabilidad civil, administrativa o penal.

   d) Proteger la inversión y el esfuerzo realizado de abusos y usos indebidos que mermen la disponibilidad o adecuación de los recursos para los fines legítimos a que se destinan.

2. Los RIC de la Universidad Alfonso X el Sabio (sistemas centrales, estaciones de trabajo, ordenadores personales, redes internas y externas, sistemas multiusuario, servicios de telefonía, de mensajería, de comunicaciones, etc.) son para el uso exclusivo de las tareas propias de la Universidad por parte de los miembros de su Comunidad o de otras personas autorizadas.

Artículo 2.- Ámbito de aplicación

1. En virtud de Lo dispuesto en el artículo anterior, la presente normativa se aplica a todas aquellas personas que hacen uso de los Sistemas Informáticos y de Comunicaciones, o que disponen de Sistemas o Redes conectadas directa o indirectamente a la red de comunicaciones de la Universidad.

2. Igualmente, el presente Reglamento se aplica íntegramente al uso que se pueda realizar a través de enlaces de datos remotos o con dispositivos portátiles, incluyendo expresamente los servicios vía web que la Universidad presta por Internet a los alumnos, a los profesores y a terceros autorizados.

3. El desconocimiento de la presente normativa no excusa de su cumplimiento.

4. El incumplimiento del presente Reglamento dará lugar a la responsabilidad administrativa, laboral, civil y/o penal que según las leyes española, resulten aplicables en dicho momento.

Título II
De la supervisión y control de los recursos

Artículo 3.- El Centro de Proceso de Datos (CPD)

El CPD es el responsable de la gestión global de la Red de Comunicaciones de la Universidad, así como de todos los Recursos y Servicios Informáticos dedicados a la Gestión Administrativa, Investigación y Docencia. Al mismo tiempo será responsable de la gestión, coordinación y administración del espacio radioeléctrico dentro de los ámbitos físicos del campus de la Universidad Alfonso X el Sabio y de sus centros asociados.

Artículo 4.- Director del Centro de Proceso de Datos (CPD)

1. En virtud de lo dispuesto en el artículo anterior, todos los Recursos Informáticos y de Comunicaciones dependen del CPD, correspondiendo al Director del mencionado Centro velar por el cumplimiento de las normas establecidas en la presente Normativa.

2. El Director del CPD, bajo sospecha o denuncia, podrá establecer medidas preventivas concretas para el cumplimiento del presente Reglamento. En cualquier caso, deberá motivar su decisión.

3. El Director del Centro de Proceso de Datos ejercerá sus funciones siguiendo las directrices de sus responsables directos en el Organigrama de la Universidad, manteniéndoles diligentemente informados de sus actuaciones.

Artículo 5.- Los Órganos de Dirección y Representación de la Universidad

1. Los Decanos y Directores de Escuela, así como los Jefes de Estudio, son responsables del buen uso de los RIC dentro de sus respectivos departamentos: ordenadores, proyectores, equipo de laboratorio, material multimedia, etc. Para ello deben asegurar la difusión y cumplimiento del presente Reglamento a todo el personal docente, investigador y auxiliar, cuya actividad coordinan, así como garantizar que los profesores vigilen el respeto a estas normas por parte de los estudiantes en las aulas y laboratorios.

2. Cada Decano o Director de Escuela designará al personal docente que considere conveniente, como Responsables de Laboratorios para garantizar la disponibilidad y buen uso de los RIC con fines docentes y de investigación.

3. No obstante a lo anterior, el Rector, Vicerrector y el Secretario General de la Universidad, deberán ser informados y en su caso, autorizar cualquier medida o solución que, en virtud de sus cargos, resulte de su competencia.

4. En el ámbito de sus competencias, el Director del Departamento de Recursos Humanos podrá también exigir el cumplimiento de la presente normativa. Además, establecerá las medidas pertinentes para facilitar su conocimiento a cada empleado de la Universidad.

5. De igual modo y en uso de sus competencias, el Gerente de la Universidad podrá también exigir el cumplimiento de la presente normativa al personal externo que preste servicio a la Universidad. Además, establecerá las medidas pertinentes para

facilitar que dichas personas conozcan y respeten la presente normativa.

Título III
De los usuarios de los recursos

Artículo 6.- El Usuario final de los recursos

1. Se entiende por usuario final a toda persona que tenga alguna vinculación con la Universidad Alfonso X el Sabio y que use los Recursos o Servicios Informáticos o de Comunicación ofrecidos por la misma.

2. El usuario final está obligado a aceptar íntegramente la presente normativa desde el momento en el que hace uso de los Recursos Informáticos o de Comunicación ofrecidos por la Universidad Alfonso X el Sabio.

3. La presente normativa se publicará permanentemente en la página web de la Universidad y se dará a conocer al usuario en el momento en que se le haga entrega de sus claves y permisos de acceso.

4. El usuario final se comprometerá a seguir las indicaciones y directrices del Centro de Proceso de Datos (CPD) en cuestiones de seguridad y buen uso.

5. La responsabilidad del uso adecuado de las herramientas informáticas, como el ordenador personal y sus programas instalados, es del usuario final. El usuario debe procurarse los conocimientos imprescindibles para el manejo de los programas que necesite.

6. El usuario final está obligado a comunicar al responsable académico (Decanos, Directores de Escuela o Jefes de Estudio) cualquier cambio en la titularidad del recurso que tenga asignado. Mientras esta notificación no se produzca, seguirá siendo el único responsable, a todos los efectos, del uso que se dé a aquel recurso y de los perjuicios que puedan derivarse del mismo, independientemente de que su relación con la Universidad haya finalizado.

7. El Director del CPD, puede denegar de manera preventiva y provisional, el acceso de un usuario a los Recursos Informáticos y de Comunicaciones de la Universidad.

Artículo 7.- Derechos del Usuario Final

Los usuarios de los servicios de informática y comunicaciones de la Universidad Alfonso X el Sabio tienen los siguientes derechos:

1. Derecho a las prestaciones reconocidas en las normas reguladoras del servicio, en las condiciones de calidad establecidas en las mismas y de acuerdo con el principio de acceso a recursos compartidos.
2. Derecho a ser informado con claridad de cualquier incidencia que sufra.
3. Derecho a ser informado con antelación de la indisponibilidad del servicio.
4. Derecho a remitir sugerencias, reclamaciones o quejas a los responsables del servicio, y a recibir respuesta en un plazo razonable.
5. Derecho a la privacidad y a la defensa de su intimidad, en cuanto usuario del servicio, con arreglo a los principios establecidos en esta normativa.

Artículo 8.- Obligaciones del usuario final

1. Los usuarios, deberán utilizar con la debida diligencia todos los equipos informáticos, así como toda la infraestructura complementaria. De igual modo, deberán evitar realizar cualquier acción, que de forma voluntaria o no, pueda dañar la integridad física de la instalación (destrozos, sustracción, traslados no autorizados, desensamblado, desconfiguración, etc.).
2. Los usuarios deberán utilizar los RIC únicamente para fines institucionales y profesionales como herramientas de apoyo. En particular:
    - Salvo autorización expresa, los usuarios no tendrán privilegio de administración sobre los equipos.
    - Los usuarios deberán facilitar al personal de soporte técnico el acceso a sus equipos para labores de reparación, instalación o mantenimiento.
    - No extraerá información en soportes o por medios electrónicos, salvo que cuente con autorización para ello, tomando especiales precauciones en caso de que se trate de información sensible, confidencial o protegida.
    - Deberá cerrar su cuenta al terminar la sesión o bloquear el equipo cuando lo deje desatendido.
    - No está permitido el uso intensivo de recursos de proceso, memoria, almacenamiento o comunicaciones, salvo necesidad manifiesta o la degradación de los servicios por cualquier medio.
3. Es responsabilidad del usuario custodiar las credenciales que se le proporcionen y evitar el acceso a ellas por terceros.
4. Evitar y prevenir la destrucción o modificación no autorizada de la información y el deterioro del trabajo de otras personas.
5. Proteger la intimidad de los demás usuarios, el secreto de las comunicaciones y el derecho a la protección de los datos personales.
6. Ni incurrir deliberadamente en actividades ilícitas de ningún tipo.
7. Los usuarios deberán notificar a la mayor brevedad posible, cualquier comportamiento anómalo de sus equipos o de otros usuarios, especialmente cuando existan sospechas de que se haya producido algún incidente de seguridad en el mismo.

8. El CPD establecerá las normativas específicas, los protocolos y los procedimientos para solicitar el acceso y el uso de los servicios.

9. Los RIC de la Universidad son un bien compartido por la comunidad universitaria, cuya finalidad es almacenar y tratar información de índole estrictamente académica, docente o investigadora, así como la derivada de la propia gestión interna de la Universidad, todo ello bajo el marco legal correspondiente.

10. Por razones de seguridad u operatividad el CPD podrá, con carácter ordinario, realizar un seguimiento estadístico del uso de las cuentas de los usuarios de los RIC.

11. En cumplimiento de la presente normativa y las restantes normas vigentes, el Director del CPD podrá realizar seguimientos específicos respecto al uso de los recursos. No obstante a lo anterior, deberá justificarlo ante sus responsables jerárquicos.

Artículo 8 bis.- Usos específicamente prohibidos

Están terminantemente prohibidos los siguientes comportamientos:

1. Utilización de cualquier tipo de software dañino.

2. Utilización de programas que, por su naturaleza, hagan un uso abusivo de la red.
3. Conexión a la red informática corporativa de cualquier equipo o dispositivo no facilitado por UAX, sin la previa autorización del Director del CPD.
4. Utilización de conexiones y medios inalámbricos con tecnologías WiFi, Bluetooth o infrarrojos que no estén debidamente autorizados por la UAX.
5. Instalación y/o utilización de programas o contenidos que vulneren la legislación vigente en materia de Propiedad Intelectual. Este comportamiento estará sometido a las previsiones disciplinarias, administrativas, civiles o penales descritas en las leyes.

Título IV
Del personal de la Universidad

Artículo 9.- Concepto

A los efectos del presente Reglamento, se entenderá por personal de la Universidad a toda aquella persona que con motivo de sus funciones profesionales, en su calidad de profesor, personal de administración y servicios o colaborador externo, tengan acceso a sus Recursos Informáticos y de Comunicaciones de la Universidad.

El personal de la Universidad tendrá las obligaciones concretas que se detallas en los artículos siguientes.

Artículo 10.- Conocimiento de la legislación de protección de datos de carácter personal

Todo usuario con acceso a Servicios de Información de la Universidad tiene la obligación de conocer la legislación de protección de datos de carácter personal y las normativas, protocolos, circulares y notificaciones internas que el CPD difunda a este respecto.

Artículo 11.- Protección de la confidencialidad de los datos personales

1. El usuario de los servicios informáticos y de comunicaciones de la Universidad no está autorizado a divulgar ni a transferir a terceros la información a la que tenga acceso como consecuencia del uso de los sistemas informáticos o documentales de la Universidad, ni a incorporarla a redes nacionales o internacionales de transmisión de datos, sin la autorización previa y expresa de la misma.

2. En particular, no facilitará copia de todo o parte de los documentos y/o datos personales de los alumnos, los datos personales de los trabajadores y/o los datos personales de colaboradores a los que en su caso pudiera tener acceso.
3. A modo enunciativo, pero no limitativo, se tendrá especial cuidado en no facilitar listados de datos personales, y en no facilitar datos personales si no es para un propósito claramente vinculado a la gestión académica o económica. Cualquier entrega de un listado a una entidad externa a la Universidad, no prevista y documentada en los procedimientos habituales, requiere la autorización expresa del Director del CPD y comunicación escrita a los responsables jurídicos de la Universidad. Esto se aplica también a los datos de acceso a internet, uso del teléfono, correo electrónico, sistemas de comunicación interna, mensajería, etc.

4. Si un profesor, un miembro del personal de administración o servicios, o un tercero autorizado por la Universidad, por razón de sus atribuciones tuviera acceso a cualquier fase del tratamiento de los datos de carácter personal, estará obligado al secreto respecto de los mismos y al deber de guardarlos con la debida diligencia. Quedará obligado asimismo a mantener dicho deber de confidencialidad aún después de finalizar sus relaciones con la Universidad.

5. Los usuarios están obligados a comunicar y denunciar ante el Director del CPD cualquier actividad que suponga la infracción de esta normativa o de la legislación vigente que en su caso resulte aplicable, desde el mismo momento en que tengan noticia de haberse producido aquélla. Se informará inmediatamente al Rector de la Universidad sobre cualquier anomalía grave que se observe acerca de la protección de la confidencialidad de los datos.

Artículo 11 bis.- Protección de la información

1. La información almacenada y tratada mediante los RIC de la UAX es de su exclusiva propiedad o responsabilidad.
2. Los usuarios tendrán acceso a la información en base a los principios de mínimo privilegio posible y necesidad de conocer, previa autorización, que necesiten para la ejecución de sus tareas, y deberán mantener sobre ella, por tiempo indefinido, una absoluta reserva.
3. Toda la información contenida en los RIC de la UAX o que circule por sus redes de comunicaciones debe ser utilizada únicamente para el cumplimiento de las funciones encomendadas a los usuarios.
4. Los usuarios deben abstenerse de comunicar, divulgar, distribuir o poner en conocimiento o al alcance de terceros (externos o internos no autorizados) la información a la que tengan acceso, salvo autorización expresa de la UAX.
5. Los usuarios tienen prohibido acceder a información perteneciente a otros usuarios o grupos de usuarios para los que no se posea autorización.
6. No está permitido almacenar información privada, de cualquier naturaleza, en los recursos de almacenamientos compartidos o locales, salvo autorización previa de la UAX.
7. No está permitido transmitir o alojar información sensible, confidencial o protegida de la UAX en servidores externos la UAX salvo autorización expresa.
8. Está absolutamente prohibido el envío al exterior de información, electrónicamente, mediante soportes informáticos o por cualquier otro medio, que no hubiere sido previamente autorizada.
9. La información almacenada de forma local en los equipos de usuario no será objeto de salvaguarda mediante ningún procedimiento corporativo de copia de seguridad, por lo tanto se recomienda utilizar las unidades de red disponibles.
10. La UAX cuenta con una política de copias de seguridad de los ficheros del sistema de almacenamiento en red (carpetas del servidor) y del resto de sistemas corporativos.

Artículo 12.- Deber de asegurar la integridad y disponibilidad de los datos

El personal del CPD vigilará y cuidará la integridad y disponibilidad de los datos, así como el suministro eléctrico de los sistemas informáticos y de comunicaciones, procurando en la medida de lo posible las condiciones óptimas de funcionamiento.

No obstante a lo anterior, el CPD informará inmediatamente de cualquier incidencia que ponga en peligro la integridad o disponibilidad de los datos.

Artículo 13.- Deber de proteger el acceso a los recursos

1. Como medidas preventivas y de seguridad, se cerrarán las puertas de acceso al CPD, a los armarios y cuartos de comunicaciones, a las aulas de ordenadores y a los laboratorios cuando no haya personal responsable presente; se informará al personal de los Servicios de Seguridad del Campus o de los centros asociados de cualquier anomalía o dificultad para cerrar o vigilar los espacios en que se sitúan los servidores

donde se almacena la información.

2. El CPD administrará cuidadosamente los sistemas de claves, y se informará inmediatamente de cualquier incidencia con claves individuales o colectivas.

Artículo 14.- Obligación de asegurar el cumplimiento de la normativa

1. Todo el Personal de Administración y Servicios está obligado a participar en la difusión de esta normativa, en ayudar al personal de reciente contratación y al profesorado y personal investigador a utilizar los Recursos Informáticos y de Comunicaciones de manera adecuada.

2. El personal de la Universidad deberá alertar al CPD, a las autoridades académicas de las que dependa y en su caso, a los órganos de administración de la Universidad, de cualquier infracción que observe.

Título V
De la utilización de los recursos

Articulo 15.- Ordenadores Personales

1. Los usuarios que utilicen ordenadores personales de su propiedad deberán mantener instaladas en sus equipos herramientas antivirus debidamente actualizadas. El CPD realiza dicha labor en los equipos que son propiedad de la Universidad.

2. Los usuarios que utilicen ordenadores personales de su propiedad, serán los responsables únicos de las licencias de software de los programas que utilicen, así como de los contenidos y archivos que se almacenen en los mismos.

3. La asistencia técnica que presta el CPD está exclusivamente dirigida a aquellos equipos que sean propiedad de la Universidad.

4. El personal del CPD podrá inspeccionar la configuración de todo dispositivo que se conecte a las redes de la Universidad, siempre que lo estime conveniente para garantizar la seguridad y buena operación de los sistemas. Si se trata de dispositivos propiedad de terceros, el usuario del mismo deberá facilitar la referida inspección, pero siempre en presencia del propietario.

5. En los supuestos en los que el usuario se niegue a facilitar dicha inspección, el Director del CPD podrá restringir o prohibir como medida preventiva, el acceso a las redes de comunicación de la Universidad.

Artículo 16.- Conexiones a la red de datos de la Universidad

Las tomas de conexión de red en las instalaciones de la Universidad no pueden ser utilizadas sin el conocimiento y autorización del Director del CPD. No está permitido conectar dispositivos repetidores ni concentradores, de cable o inalámbricos, sin la autorización expresa del Director del CPD y previa supervisión por parte de personal técnico del CPD.

Artículo 17.- Telefonía

El servicio telefónico de la Universidad está sujeto íntegramente a la presente Normativa. Los usuarios no podrán utilizar los servicios telefónicos de la Universidad para usos distintos a los

que motivaron su adjudicación. En caso de utilización indebida, se podrá exigir el resarcimiento de los daños y perjuicios económicos que se hubieran causado.

Artículo 18.- Espacio radioeléctrico

1. Las comunicaciones inalámbricas dentro de los recintos propiedad de la Universidad y de sus centros asociados están sujetas a la presente normativa.

2. El uso de telefonía móvil en bandas públicas está permitido en las zonas en que no se prohíba expresamente. Salvo autorización expresa, no está permitido el uso de telefonía móvil en espacios dotados con instrumental médico, bibliotecas y zonas de estudio.

3. El CPD administrará en última instancia, las bandas de 2,4 GHz y 5GHz destinadas a usos industriales y de investigación dentro de los recintos propiedad de la Universidad y de sus centros asociados.

Artículo 19.- Cuentas informáticas y clave secreta

1. Las cuentas de usuarios en los sistemas informáticos de la Universidad Alfonso X el Sabio son personales e intransferibles y de uso exclusivo en el ámbito académico, de investigación o de la gestión administrativa de la Universidad.

2. Es responsabilidad de cada usuario observar la mayor diligencia respecto a la utilización de las claves de acceso a los servicios. Queda prohibida la divulgación de las claves de acceso personales de cada usuario.

3. En virtud de lo anterior, el usuario tiene un deber de secreto de las claves que se le adjudiquen para desempeñar sus funciones. Además, usará claves que no sean triviales o simples de averiguar, la cambiará periódicamente y siempre que crea o sospeche que su confidencialidad pueda ser violada. Estos criterios se extienden igualmente a las claves de servicios o sistemas a los que tenga acceso en función de su actividad.

Artículo 20.- Correo electrónico de la Universidad

El uso de las cuentas de correo electrónico facilitadas a los usuarios por el CPD, se ajustará a las siguientes normas concretas:

1. El correo electrónico @uax.es y @alum.uax.es, será el medio oficial de comunicación corporativa interna y no puede ser ignorado ni manipulado. Será el medio utilizado para la comunicación y notificación de los documentos relativos a los expedientes disciplinarios sancionadores que pudieran sustanciarse por la comisión de faltas disciplinarias, de conformidad con el Reglamento de Disciplina Académica de la Universidad Alfonso X el Sabio.

2. El usuario final es responsable de comunicar de inmediato al CPD toda dificultad de acceso a su correo.

3. Como recurso dispuesto por la Universidad para soporte de su actividad académica, investigadora, administrativa y empresarial, no debe ser utilizado para otros fines que los razonablemente relacionados con la actividad universitaria.

4. La Universidad no es responsable del contenido de las comunicaciones emitidas por el usuario final a través del correo electrónico, ni del contenido de correos que el usuario

final pueda recibir, aparte de aquellos emitidos por la propia autoridad académica o administrativa.

5. El usuario final se compromete a proteger la imagen y el buen nombre de la Universidad Alfonso X el Sabio en todas sus comunicaciones por correo electrónico.

6. El usuario evitará la difusión por correo electrónico de contenidos ilegales u ofensivos, así como la proliferación de correo comercial no solicitado y la difusión de virus informáticos. Así mismo, evitará la difusión de archivos anexos de contenido lúdico (películas, música, imágenes, juegos) que por su gran tamaño saturan la capacidad del servicio y merman su disponibilidad para los fines a que originalmente está destinado.

7. El CPD establecerá los mecanismos de acceso, las facilidades y complementos para su uso, y las limitaciones del servicio de correo electrónico.

Artículo 21.- Acceso a Internet

1. La Universidad facilita, en la mayor parte de los ordenadores de sus instalaciones, acceso a la red Internet a través de diversos protocolos de comunicación. El usuario que accede a Internet utilizando los recursos de la Universidad ha de cumplir la presente normativa, así como la legislación estatal vigente.

2. Bajo indicios de sospecha o denuncia, la Universidad podrá analizar las trazas de navegación por Internet de los usuarios, con el fin de evitar el incumplimiento de esta normativa.

3. El CPD establecerá los filtros limitativos que estime necesarios para garantizar la seguridad y el buen uso de los accesos a Internet conforme a esta Normativa.

Artículo 22.- Supervisión y control de las comunicaciones electrónicas

1. En cumplimiento de la legislación vigente, la Universidad está obligada a conservar ciertos datos para la utilización en el marco de una investigación criminal o para la salvaguardia de la seguridad pública y la defensa nacional, poniéndose a disposición de los Jueces o Tribunales o del Ministerio Fiscal que así los requieran.

2. La comunicación de estos datos a las Fuerzas y Cuerpos de Seguridad se hará con sujeción a lo dispuesto en la normativa sobre protección de datos personales.

3. En virtud de lo anterior, el CPD retendrá por un periodo de un año todas las trazas de correo electrónico y acceso a Internet (consistentes en identificador de la máquina y usuario, fecha, origen y destino). En ningún caso la obligación de retención de datos afectará al secreto de las comunicaciones.

Artículo 23.- Principio de economía

1. La capacidad de transmisión de datos de las redes informáticas es limitada. Los usuarios finales tienen la obligación de utilizar la red de datos con economía, siendo conscientes de que al tratarse de un recurso compartido, cualquier uso abusivo puede conllevar la saturación y merma de disponibilidad del servicio para los restantes usuarios.

2. Por dicho motivo, se prohíben las transferencias de datos excesivas o muy voluminosas, de carácter no justificado, o que puedan comprometer la normal

actividad de la Universidad. La presente norma incluye la sintonización de emisoras de radio o de televisión a través de Internet, así como la descarga o distribución de materiales de audio y video de uso personal.

Artículo 24.- Bienes fungibles

El papel, los cartuchos de tinta para las impresoras, los disquetes, cintas de datos y en general, todos los materiales considerados como consumibles informáticos, han de ser administrados por cada usuario final con lealtad y responsabilidad, aplicando el principio de economía y conforme a los fines legítimos para la actividad universitaria.

Artículo 25.- Residencias Universitarias

1. Con el fin de facilitar a los usuarios de las Residencias las mejores oportunidades en su desarrollo académico, la Universidad facilita el acceso a determinados servicios informáticos de comunicaciones desde sus habitaciones.

2. El uso de los RIC en las Residencias Universitarias está sujeto íntegramente a esta normativa. Los estudiantes residentes que deseen acceder a dichos recursos aceptan explícitamente respetarla como requisito indispensable para disponer del acceso a los mismos.

3. Los servicios ofrecidos a las Residencias son determinados anualmente por el Gerente de la Universidad, a propuesta del Director del CPD, en función de la disponibilidad e idoneidad de los recursos a compartir. La Dirección de las Residencias establecerá, a propuesta del CPD, las normas reguladoras del uso de estos servicios en las Residencias Universitarias.

Artículo 25 bis - Equipos Portátiles y Móviles

1. Este tipo de dispositivos estará bajo la custodia del usuario que los utilice y deberá adoptar las medidas necesarias para evitar daños o sustracción, así como el acceso a ellos por parte de terceros no autorizados.
2. La pérdida o sustracción de estos equipos se ha de poner inmediatamente en conocimiento de la UAX para la adopción de las medidas que correspondan y a efectos de baja en el inventario.
3. Los usuarios no tendrán privilegio de administración sobre los equipos portátiles y no podrán realizar ninguna modificación hardware/software sobre los mismos.
4. Los equipos portátiles y móviles deberán utilizarse únicamente para fines institucionales, especialmente cuando se usen fuera de las instalaciones de la UAX.
5. Debe evitarse la conexión a redes públicas externas.
6. Los usuarios de equipos portátiles deberán realizar conexiones periódicas a la red corporativa, para permitir la actualización de las aplicaciones y medidas de seguridad instaladas.

Artículo 25 ter - Uso de Soportes USB o Magnéticos

1. Los soportes están destinadas a un uso exclusivamente profesional, como herramienta de transporte de ficheros, no como herramienta de almacenamiento. La UAX podrá poner a disposición de los usuarios de aplicaciones, servicios y unidades de almacenamiento en red, que podrán usarse para tal propósito.
2. Este tipo de dispositivos estará bajo la custodia del usuario que los utilice y deberá

adoptar las medidas necesarias para evitar daños o sustracción, así como el acceso a ellos por parte de terceros no autorizados.

3. La pérdida o sustracción de una memoria USB, con indicación de su contenido, deberá ponerse en conocimiento de la UAX, de forma inmediata.
4. Los medios de almacenamiento que, por obsolescencia o degradación, pierdan su utilidad, y especialmente aquellos que contengan información sensible, confidencial o protegida, deberán ser eliminados de forma segura para evitar accesos ulteriores a dicha información para lo cual se solicitará mediante la herramienta de gestión de incidencias al CPD.

Artículo 25 quater- Copias de Seguridad

1. De forma periódica, se realizarán copias de seguridad, tanto completas como incrementales, de las unidades de red compartidas de la UAX donde se almacene la información. En ningún caso se realizará copia de seguridad de la información almacenada de forma local en el puesto del usuario.
2. La información almacenada en las copias de seguridad podrá ser recuperada en caso de que se produzca algún incidente. Para recuperar esta información el usuario habrá de solicitarlo mediante la herramienta de gestión de incidencias.

Artículo 25 quinquies - Protección de la Documentación Impresa

1. La documentación impresa que contenga datos sensibles, confidenciales o protegidos, debe ser especialmente resguardada, de forma que sólo tenga acceso a ella el personal autorizado, debiendo ser recogida rápidamente de las impresoras y fotocopiadoras y ser custodiada en armarios bajo llave.
2. Cuando concluya la vida útil de los documentos impresos con información sensible, confidencial o protegida, deberán ser eliminados en las máquinas destructoras de la UAX, de forma que no sea recuperable la información que pudieran contener.
3. Por razones ecológicas y de seguridad, antes de imprimir documentos, el usuario debe asegurarse de que es absolutamente necesario hacerlo.

Artículo 25 sexies - Impresoras, Escáneres, Fotocopiadoras y Faxes

1. En ningún caso el usuario podrá hacer uso de impresoras, escáneres, fotocopiadoras o equipos de fax que no hayan sido proporcionados por la UAX y, en su consecuencia, estén debidamente configurados.
2. Cuando se usen estos equipos, la documentación deberá permanecer el menor tiempo posible en las bandejas de entrada o de salida, para evitar que terceras personas puedan acceder a la misma.
3. Cuando se digitalicen documentos el usuario deberá ser especialmente cuidadoso con la selección del directorio compartido donde habrán de almacenarse las imágenes obtenidas, especialmente si contienen información sensible, confidencial o protegida.
4. Si se encontrase documentación sensible, confidencial o protegida abandonada en una fotocopiadora o impresora, el usuario intentará localizar a su propietario para que éste la recoja inmediatamente. Caso de desconocer a su propietario o no localizarlo, lo pondrá inmediatamente en conocimiento del Responsable de Seguridad.

Artículo 25 septies - Protección de la Propiedad Intelectual

1. Está estrictamente prohibida la ejecución de programas informáticos en los Sistemas de Información de la UAX sin la correspondiente licencia de uso.

2. Los programas informáticos propiedad de la UAX o licenciados la misma están protegidos por la vigente legislación sobre Propiedad Intelectual y, por tanto, está estrictamente prohibida su reproducción, modificación, cesión, transformación o comunicación, salvo que los términos del licenciamiento lo permitan y con la autorización previa de la UAX.
3. Análogamente, está estrictamente prohibido el uso, reproducción, cesión, transformación o comunicación pública de cualquier otro tipo de obra protegida por derechos de Propiedad Intelectual, sin la debida autorización de la UAX.

Artículo 25 octies - Incidencias de seguridad

Cuando un usuario detecte cualquier anomalía o incidencia de seguridad que pueda comprometer el buen uso y funcionamiento de los RIC de la UAX o su imagen, deberá informar inmediatamente al Responsable de Seguridad, que lo registrará debidamente y elevará, en su caso.

Título VI
De las infracciones y sanciones

Artículo 26.- Infracciones

Se considera incumplimiento de las condiciones de uso de los Recursos de Informática y Comunicaciones, de manera enunciativa pero no limitativa, los siguientes supuestos:

1. Los usos ilícitos, por parte de terceras personas, de cuentas de usuarios (usuario/contraseña) en los sistemas informáticos tengan o no conocimiento de ello los usuarios autorizados, así como, el incumplimiento de los términos de licencias del software genérico adquirido en la Universidad. La responsabilidad se extiende tanto a quien realiza el acceso indebido como al responsable de la cuenta.
2. La búsqueda de palabras clave de otros usuarios o cualquier intento de encontrar y explotar fallos en la seguridad de los sistemas informáticos de la Universidad Alfonso X el Sabio o de otras entidades o personas, o el hacer uso de aquellos sistemas para atacar cualquier sistema informático.
3. La creación, uso o almacenamiento de programas o de información que pueden ser utilizados para atacar los sistemas informáticos de la Universidad Alfonso X el Sabio u otros externos, salvo aquellas personas expresamente autorizadas a realizar dichas labores conducentes a garantizar la seguridad y operatividad de los servicios de la red UAX.
4. La introducción intencionada de virus, caballos de Troya, gusanos, bombas de tiempo, robots, arañas, anonimizadores o cualquier otro software perjudicial o nocivo.
5. El destrozo, sustracción o el traslado no autorizado a otras dependencias de cualquier elemento físico de la instalación informática o de la infraestructura complementaria.
6. La alteración de la integridad, y el uso o manipulación indebida de los datos a que se tiene acceso.
7. La instalación y utilización de aplicaciones informáticas sin licencia.
8. Gestionar o administrar actividades con ánimo de lucro.
9. La instalación y utilización de juegos de ordenador, juegos en línea o juegos de azar de cualquier tipo.
10. La descarga o distribución de documentos, libros, imágenes, películas o música infringiendo los derechos de autor y de copia.

11. El uso indebido de los servicios de la red UAX (correo electrónico, mensajería interactiva, www, etc.) para comunicarse con otros usuarios de los sistemas informáticos de la red de la Universidad o a las redes que la Universidad está conectada, cuando:

    a) Difundan contenidos atentatorios contra los principios enunciados en los Estatutos de la Universidad.

    b) Consistan en actividades ilícitas o ilegales de cualquier tipo y, particularmente, en difundir contenidos o propaganda de carácter racista, xenófobo, pornográfico, sexista, de apología del terrorismo o atentatoria contra los derechos humanos; o en actuar en perjuicio de los derechos a la intimidad, al honor, a la propia imagen o contra la dignidad de las personas

    c) Posibiliten suplantaciones de direcciones de la red.

    d) Se dirijan a recopilar información sobre terceros, incluidas sus direcciones de correo electrónico, sin el consentimiento de los interesados.

    e) Se concreten en la creación de identidades falsas con el fin de engañar a terceros respecto de la identidad del remitente o del origen de un mensaje.

    f) Se lleven a cabo con fines propagandísticos y comerciales, sin autorización expresa.

    g) Difundan intencionadamente manifestaciones o referencias falsas, incorrectas o inexactas acerca de la Universidad Alfonso X el Sabio.

12. No mantener los Recursos Informáticos bajo su responsabilidad con las medidas de seguridad necesarias.

13. No comunicar al CPD o a la autoridad académica las infracciones a esta normativa.

14. Utilizar comunicaciones móviles personales para establecer vínculos o pasarelas entre los sistemas de la Universidad y redes o sistemas externos.

Artículo 27.- Medidas preventivas y sancionadoras

1. El incumplimiento de la presente normativa supondrá, de forma preventiva e inmediata, la suspensión del servicio prestado y/o el bloqueo temporal de los sistemas, cuentas o redes de la UAX y a los que tiene acceso el usuario, con el fin de garantizar el buen funcionamiento de los servicios. El CPD asumirá la responsabilidad de esta suspensión temporal y la comunicará a los responsables administrativos y académicos encargados de la resolución del incidente.

2. El causante de cualquier daño en el equipamiento de los sistemas informáticos o de comunicaciones será, en todo caso, responsable civilmente del mismo y se obliga, en consecuencia, a resarcir de inmediato a la Universidad los perjuicios ocasionados.

3. Ante cualquier infracción, la Universidad se reserva el derecho de aplicación de las medidas disciplinarias que considere oportunas, de acuerdo con su régimen disciplinario interno, sus estatutos y su régimen laboral.

4. La Universidad pondrá en conocimiento de la autoridad judicial y de las fuerzas de

seguridad del Estado aquellas infracciones que presuma constitutivas de delito contra la legislación vigente o contra los legítimos intereses de la Universidad.

DISPOSICIONES FINALES

PRIMERA.- Las diferencias de interpretación que pudieran surgir en el ámbito de aplicación de esta normativa serán resueltas por el Director del Centro de Proceso de Datos, y en última instancia, por el Rector de la Universidad.

SEGUNDA.- La Universidad desarrollará los reglamentos complementarios a esta normativa que considere oportunos para las distintas áreas de actividad, dándolos a conocer a la comunidad universitaria a través su página web y del correo electrónico. De la misma manera se darán a conocer las sucesivas versiones o revisiones de esta normativa que aconsejarán sin duda en el futuro el devenir de la tecnología y de los usos aceptables de los recursos informáticos y de comunicaciones.

TERCERA.- Se faculta al Director del Centro de Proceso de Datos par que, previa audiencia de los respectivos representantes de los órganos dirección y representación de la Universidad expuestos en el artículo 5, desarrolle los procedimientos necesarios para lograr el cumplimiento del presente Reglamento.