# CIRCULAR Nº 1 SOBRE POLÍTICA DE USO DE LOS RECURSOS INFORMÁTICOS Y DE LA INFRAESTRUCTURA DE RED EN EL C.S.I.C.

## 1. ASPECTOS GENERALES:

Los ordenadores y la red proporcionan acceso y recursos, dentro y fuera del ámbito del CSIC, y nos permiten la comunicación con usuarios en todo el mundo. Este privilegio acarrea unas responsabilidades a los usuarios, que han de respetar los derechos de los otros usuarios, la integridad del sistema y de los recursos físicos y respetar las leyes y regulaciones vigentes.

Los motivos que han llevado a la redacción de esta política, han sido:

**Necesidad:** Los usuarios de los recursos informáticos y de las redes de los diferentes Centros y/o Institutos del CSIC son responsables de no abusar de estos recursos y de mantener el respeto a los derechos del resto de usuarios. Esta política aporta una serie de recomendaciones y líneas de actuación para distinguir entre el uso correcto de los sistemas de información y el indebido.

**Objetivos de la Política:** El objetivo que se plantea es asegurar una infraestructura informática que facilite la realización de las misiones básicas de los Centros, Institutos y Unidades Asociadas del CSIC, como son la investigación y las tareas administrativas. Los ordenadores, servidores y redes son tecnologías que permiten de forma eficiente el acceso y distribución de información y conocimiento, originado tanto en el CSIC como en cualquier otro lugar. Como tales, se consideran una infraestructura estratégica para el desarrollo de los objetivos del CSIC. Además, ya que estas tecnologías nos permiten la posibilidad de acceder, copiar y compartir información con fuentes remotas, nuestros usuarios deben ser conscientes de los derechos de los otros, tales como su privacidad o protección de la propiedad intelectual. Esta política explica qué se considera un uso apropiado de las redes y sistemas con relación a los derechos de otros. Finalmente también se hará una enumeración de las responsabilidades que supone el uso de estos recursos y las consecuencias de su abuso.

**Resumen:** Los usuarios de nuestras redes 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 en exceso recursos compartidos con el resto de usuarios y respetar las políticas de

licencias de software. Esta política se debe aplicar a nuestras redes, a todos los equipos conectados a ella y a toda la información contenida en estos equipos.

## 2. ÁMBITO DE APLICACIÓN:

### 2.1. Agentes a los que se aplica esta política:

Esta política será de aplicación para todos los miembros del CSIC, ya sea a nivel individual (investigadores, personal de apoyo, personal de administración, equipo directivo, becarios de investigación, personal vinculado a proyectos de investigación, etc.) o colectivo (Centros, Institutos, Departamentos, Grupos, etc.) en cuanto a que hagan uso de los recursos expuestos en el siguiente apartado.
También se aplicará a cualquier otra entidad externa que utilice los recursos informáticos de la Institución.

### 2.2. Recursos a los que se refiere esta política:

Se incluyen aquí todos los sistemas de información del CSIC, ya sean individuales o compartidos y estén o no conectados a nuestras redes. Se aplicará a todos los equipos (estaciones de trabajo, PC's y servidores) e infraestructura de comunicaciones que sean propiedad o estén administrados por el CSIC, así como aquellos equipos que se conecten a través de una extranet a las redes de la Institución.

Todo esto incluye terminales, ordenadores personales, estaciones de trabajo, servidores y periféricos asociados, así como el software, independientemente de que se use para gestión administrativa, económica, investigación u otros.

Los Centros e Institutos deberán disponer de unas normas de actuación que regulen el proceso de altas y bajas de usuarios para acceder a los recursos.

### 2.3. Políticas especificas y locales:

El presente documento es un marco que define una política global de uso para todos los recursos del CSIC. De forma específica se podrán articular dentro de este marco **políticas y recomendaciones de buen uso de servicios e infraestructuras, como pueden ser:**

- Servicios telemáticos (correo electrónico, Web, multimedia, etc.).
- Buen uso de la infraestructura de redes y del acceso a Internet.
- Acceso a servidores con datos de carácter personal.
- Incidencias de seguridad.

Los distintos Centros e Institutos del CSIC podrán definir también sus "políticas locales" o condiciones de uso para los recursos informáticos que estén bajo su control, las cuales deberán ser congruentes con esta política general. Los responsables informáticos y directores de Centros, Institutos o Unidades Asociadas serán los encargados de la difusión de las mismas.

Cuando sea necesario el uso de infraestructuras de red externas (como en nuestro caso lo es RedIRIS o en algunos casos, también, la Red Telemática de la Comunidad Autónoma), las políticas de estas instituciones serán de aplicación en nuestras redes.

### 2.4. Aspectos legales:

Son de aplicación las leyes y normativa españolas, así como las que dimanen de la Unión Europea y de las comunidades autonómicas en relación con protección de datos personales, propiedad intelectual y uso de herramientas telemáticas, así como las que puedan aparecer, en un futuro, a este respecto. Por todo ello, el CSIC podrá ser requerido por los órganos administrativos pertinentes a proporcionar los registros electrónicos o cualquier otra información relativa al uso de los sistemas de información.

Esta política se sitúa dentro del marco jurídico definido por las leyes y reales decretos siguientes:

- *Ley Orgánica de Protección de Datos (15/1999).*
- *Ley Orgánica 1/1982, de 5 de mayo, de Protección Civil del Derecho al Honor, a la intimidad Personal y Familiar y a la Propia Imagen.*
- *Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.*
- *Real Decreto 994/1999: Reglamento de medidas de seguridad de los ficheros automatizados que contienen datos de carácter personal.*
- *Real Decreto 263/1996: Utilización de técnicas electrónicas, informáticas y telemáticas por la Administración General del estado.*

## 3. DEFINICIONES

**Responsable Administrativo:** Es el responsable de los equipos informáticos que haya instalados en un Centro o Instituto, esta responsabilidad se limita a autorizar la instalación de los mismos, quién puede utilizarlos y qué uso se hace de ellos. Normalmente el responsable Administrativo es el Director del Centro o Instituto o la persona que él delegue.

**Administrador de Sistemas:** Es el responsable de la gestión y administración de los equipos informáticos y de supervisar el cumplimiento de la política de uso de los mismos. Será normalmente el informático del Centro o Instituto.

**Responsable Administrativo de los recursos informáticos del CSIC:** Esta responsabilidad será de la Vicepresidencia de Investigación Científica y Técnica.

**Usuarios:** Toda persona que utilice los recursos informáticos del CSIC.

**Responsable de seguridad:** Será quien se debe encargar de dirigir las medidas y acciones para hacer cumplir esta política, así como de su

interpretación, control de cumplimiento y resolución de los problemas relativos a la misma.

## 4. POLÍTICAS 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 del CSIC. 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 de los Directores de los Centros, Institutos o Unidades Asociadas dar la difusión necesaria a esta política para que sea conocida por todos los agentes a los que se aplica.

### 4.1. Sobre la integridad y disponibilidad de los recursos:

Los usuarios deben respetar la integridad de los recursos y sistemas de información. Para ello se enumeran una serie de recomendaciones:

- Un usuario no debe tratar de alterar o eliminar ordenadores (hardware o configuración del SO), software o periféricos que estén asignados a otros usuarios, sin la debida autorización.
- Los usuarios no deberán entorpecer o absorber recursos compartidos de forma tal que impidan a otros realizar sus tareas de una forma eficiente. Esto incluye, al menos, lo siguiente:
  - El envío a través de correo electrónico de cartas encadenadas o mensajes excesivamente voluminosos o con muchos destinatarios, ya sean locales o ajenos a la Institución.
  - Uso de programas que puedan saturar los servidores o las redes de los Centros, Institutos o Unidades Asociadas del CSIC, cuando haya alternativas más eficientes o no tengan una prioridad alta. En cualquier caso, se beberá solicitar con la suficiente antelación al responsable informático
  - Modificación no autorizada de privilegios o permisos.
  - Intentos de desactivar servidores o cortar el funcionamiento de las redes.
  - Intento de realizar cualquier tipo de daño (físico o lógico) a las herramientas informáticas del CSIC: equipos, aplicaciones, documentos, etc,...
- Los usuarios no deberán intencionadamente desarrollar o usar programas cuyo objetivo sea dañar otras máquinas o acceder a recursos restringidos (malware: virus, troyanos, puertas traseras, etc.). Más aún, deberán controlar que no se les infecte su equipo con este

tipo de software, para lo cual el responsable informático del Centro, Instituto o Unidad Asociada, donde los hubiese, o si no el CTI, deberá proporcionar las herramientas y utilidades adecuadas. El uso de este tipo de programas, contra un agente externo o contra el propio CSIC, puede incluso implicar acciones legales por la parte afectada.

- Los usuarios de las redes no deben utilizar los enlaces de red para otros usos que no sean los permitidos en las "Recomendaciones de Uso de la Red" o los propios necesarios para el desempeño de su actividad.

### 4.2. Sobre accesos no autorizados y suplantación de identidad.

Los usuarios no deben tratar de conseguir accesos a sistemas o recursos a los que no estén autorizados y tampoco permitir o facilitar que otros lo hagan.
Los usuarios deben respetar los derechos del resto de usuarios; la mayoría de los sistemas de uso compartido proporcionan mecanismos para proteger los datos e información privada de posibles consultas por parte de otros. Los intentos de saltarse estos mecanismos para conseguir accesos no autorizados a información calificada como personal supondrán una violación de esta política e incluso del marco legal señalado en el apartado 2.4.

Los administradores de sistemas que estén autorizados podrán acceder, exclusivamente, por motivos de mantenimiento y/o de seguridad, a aquellos ficheros de usuario que permitan al administrador detectar, analizar y seguir las trazas de una determinada sesión o conexión.

En cualquier caso, el administrador de sistemas tiene el deber de guardar secreto sobre el contenido de los ficheros de los usuarios, no estando autorizado a permitir que terceros puedan acceder a los mismos.

En el supuesto de que una política interna expresamente lo autorice, el administrador de sistemas podrá permitir el acceso a terceros (responsables de proyectos, directores, gerentes,...) a determinados ficheros de otros usuario, debiendo contar en todo caso, tanto con la autorización del director del Centro o Instituto como del propietario de los ficheros.

- Los usuarios de los recursos informáticos del CSIC no deben acceder a ordenadores, aplicaciones, datos o información o redes para las que no estén debidamente autorizados. Tampoco deberán permitir de forma intencionada que otros lo hagan, independientemente de que el recurso (equipo, aplicación, red, datos, etc.) pertenezca o no al CSIC.
- No está permitido realizar de forma intencionada acciones cuyo fin sea la obtención de contraseñas de otros usuarios sin el consentimiento de estos.

- Cualquier defecto o anomalía que se descubra en el sistema o en su seguridad se debe reportar con la mayor brevedad posible al responsable informático del Centro, Instituto o Unidad Asociada, o al CTI, quien será el encargado de investigar y proponer soluciones al problema.
- Todo aquel usuario que haya sido autorizado a usar una cuenta mediante un sistema de login/password será responsable de mantenerla en secreto y no darla a conocer a nadie más sin la autorización del administrador del sistema. Será siempre el responsable de lo que se ejecute en el sistema desde esa cuenta.
- Los usuarios deberán evitar el tener compartidos recursos (ficheros, directorios, etc.) sin los mecanismo de seguridad necesarios y disponibles en cada sistemas operativos y/o aplicaciones que garanticen la seguridad de su equipo y la red.

### 4.3. Sobre el uso de los servicios de comunicación y difusión de información

El correo electrónico, las listas de distribución, servicios de mensajería instantánea o foros de discusión son herramientas que facilitan la comunicación entre las personas, así como la difusión de información a varios interlocutores de una sola vez. Por ello conviene tener en cuenta una serie de comportamientos a la hora de usar estos medios.

- No se deben usar estas utilidades para el envío de mensajes con contenido fraudulento, ofensivo, obsceno o amenazante.
- Las listas de distribución de correo se deben usar sólo para enviar mensajes relacionados con la finalidad de las mismas. Existirán también listas libres, que deberán observar, no obstante, lo expuesto en el punto anterior. Podemos considerar que los usuarios se han suscrito a una lista para recibir un tipo de información y en caso de que no se respetara lo anterior el resto de los suscriptores de la lista podrían quejarse de recibir información no solicitada.
- Los recursos del CSIC no se deben usar para actividades personales que no tengan relación con las propias del desempeño laboral, salvo de forma esporádica y siempre dentro de las normas internas de cada Centro en cuanto a seguridad. En estos casos el responsable informático no está obligado a prestar soporte.
- No se deben usar estos servicios con fines comerciales, salvo autorización expresa del Órgano de gobierno competente. En cualquier caso, el uso comercial que se haga debe estar relacionado con las actividades del CSIC y suponer información relevante para la comunidad científica (convenios, ofertas especiales para el personal del CSIC, etc.).

**4.4.** Sobre uso de la infraestructura de comunicaciones

- No se podrá instalar ningún servicio telemático (Correo electrónico, Servidores Web, FTP, etc) sin la autorización expresa del responsable administrativo (Director) y con la designación de un administrador del sistema.
- No se podrá realizar la conexión, desconexión o reubicación de equipos o cambios de configuración de los mismos sin la autorización expresa del responsable administrativo (Director) o del administrador del sistema.
- Estará prohibido la instalación de dispositivos, y tarjetas de acceso remoto, módems, RDSI, ADSL, routers o cualquier otro dispositivo de comunicaciones en ordenadores o redes sin la autorización expresa del responsable administrativo (Director) o del administrador del sistema.
- Estará prohibido la conexión de equipos de comunicaciones para intercambio de información (rutas, redes,...) entre ordenadores de las redes del CSIC y otros ajenos a dichas redes.
- Estará prohibido el uso de la red y ordenadores del CSIC para conseguir acceso no autorizado a cualquier ordenador.
- Estará prohibido instalar o ejecutar en cualquier punto de la red informática (ordenadores o software de red) programas o ficheros que traten de descubrir información distinta de la del propio usuario, en cualquier elemento de la red. Esto incluye sniffer, escaneadores de puertos, etc....
- No se podrá facilitar a una tercera entidad acceso, a través de las redes del CSIC, a la infraestructura de comunicaciones propias de este organismo; es decir, no se podrá proporcionar transito a terceras instituciones, salvo obtención del consentimiento, previamente solicitado, de la Vicepresidencia de Investigación Científica y Técnica, en su calidad de responsable administrativo de los recursos informáticos del CSIC.
- Se deberá evitar la circulación de información comercial (con excepción de respuestas a peticiones expresas de información sobre productos o servicios de interés para las actividades habituales del Organismo)
- No se podrá proceder a la destrucción, manipulación o apropiación indebida de la información que circule por la red.
- Se evitará el consumo excesivo de los recursos por parte de cualquier usuario.
- Se deberá respetar el derecho de privacidad de los diferentes usuarios de la red

- La infraestructura de red del CSIC nunca deberá ser utilizada, bajo ningún concepto, para lo siguiente:
  - Transmisión de información o acto que viole la legislación vigente en el Estado Español.
  - Fines privados o personales, con o sin animo de lucro.
  - Fines lúdicos
  - Fines no estrictamente relacionados con las actividades propias del Organismo.
  - Creación o transmisión de cualquier tipo de información que sea ofensiva, obscena o indecente.
  - Transmitir información difamatoria de cualquier tipo, ya sea contra entidades o personas
  - No se podrá divulgar información que viole los derechos de propiedad intelectual.
  - No se podrá usar cualquier aplicación de la cual se sepa que su uso pueda suponer una disfunción de la red.

### 4.5. Sobre las licencias de software y "copyrights":

Los usuarios y administradores deben respetar las condiciones de licencia y copyright del software que usen en sus equipos.

- Todo software adquirido de forma central para el CSIC (licencias campus o licencias para instalación en servidores centrales) deberá estar debidamente licenciado y la responsabilidad de esto recaerá en el Director del Centro, Instituto o Unidad Asociada, o el responsable del servicio que haya autorizado su adquisición.
- Todo software que se use en el CSIC para fines administrativos o investigadores debe estar debidamente licenciado, con un número de licencias que se corresponda con el número de usuarios simultáneos. Por supuesto, podrá usarse en equipos del CSIC software "libre" (Open source, freeware, etc.).
- Todo software que se use que esté protegido por copyrights no puede ser copiado, salvo con autorización del propietario. No se podrán usar los medios que el CSIC pone a disposición de su comunidad para copiar software protegido o romper las protecciones del mismo.
- Aparte del software, toda otra información que también posea derechos de autor, que esté en formato electrónico y que haya sido obtenida de otro equipo o red, se debe usar de acuerdo con la legislación vigente.
- Los usuarios responderán siempre personalmente del software que haya instalado en sus equipos, así como del uso que del mismo se efectúe, y deberán cumplir con las obligaciones y requisitos que se deriven de su instalación y utilización.

En ningún caso los usuarios podrán permitir que ninguna persona lleve a cabo la instalación en sus equipos de software que no esté debidamente licenciado.
El incumplimiento de estas obligaciones por parte de los usuarios dará lugar a la aplicación de las medidas preventivas, correctivas y disciplinarias previstas en el presente Política y, en su caso, al ejercicio de las acciones legales pertinentes.

## 5. LOS ADMINISTRADORES DE LOS SISTEMAS Y SUS RESPONSABILIDADES:

Como se ha expuesto antes, cada usuario se hará responsable del buen uso del equipamiento y la red que el CSIC pone a su disposición. Pero hay determinados recursos (servidores, aplicaciones, bases de datos, red) cuyo uso o explotación es compartido por un grupo de usuarios. Estos recursos deberán tener un **responsable administrativo** (que asumirá competencias organizativas) y un **administrador del sistema**, que será nombrado por el responsable administrativo y que se encargará de las tareas técnicas de funcionamiento del recurso en cuestión.

Así, por ejemplo, un Centro o Instituto (como unidad organizativa del CSIC) podría disponer de los servidores que considere necesario para dar determinados servicios al personal adscrito a estos; se considerará que su **Director** será el responsable administrativo y quien nombrará a una persona (normalmente dentro del propio Centro o Instituto) para realizar las funciones de administrador de esos sistemas.

### 5.1. La administración de los recursos globales.

Corresponderá al Centro Técnico de Informática del CSIC el papel de Administrador de los Sistema para los recursos informáticos globales del CSIC. La Vicepresidencia de Investigación Científica y Técnica, de la que depende el CTI, será el responsable administrativo en el CSIC.
El administrador del sistema (en este caso, el CTI como gestor de los recursos informáticos globales del CSIC) deberá organizarse y realizar las acciones y esfuerzos necesarios para:

- Prevenir y evitar robos, pérdidas o cualquier daño físico a los componentes del sistema.
- Respetar todos los acuerdos y licencias relativos al hardware y software que sean aplicables al sistema.
- Tratar la información almacenada en el sistema de la forma apropiada y adoptar las precauciones y medidas para proteger la seguridad de los datos, red y equipos según lo especificado en el marco legal vigente y los compromisos adquiridos. Las medidas de seguridad se

dimensionarán en función de la importancia y criticidad de los recursos que se quieran proteger.
- Dar publicidad a las distintas políticas y recomendaciones de uso de servicios.
- Garantizar los procedimientos de recuperación de la información y del sistema en los servidores bajo su responsabilidad.
- Colaborar con otros administradores de sistemas de otras entidades o redes (por ejemplo, resto de organizaciones afiliadas a RedIRIS, CERTs, etc.), para resolver los problemas causados en las mismas desde máquinas bajo el dominio del CSIC.

Para hacer cumplir esta política, el administrador del sistema debe contar con los medios necesarios (herramientas y personal) y la autorización (delegada por el órgano de gobierno correspondiente) para tomar medidas razonables que garanticen el buen funcionamiento de los recursos para la colectividad y su seguridad.
El administrador del sistema puede, temporalmente y con el consentimiento (cuando sea posible) del Responsable Administrativo o del Responsable de Seguridad, suspender los privilegios de acceso o conexión si lo estima necesario o apropiado para mantener la integridad y disponibilidad del sistema o de la red.

### 5.2. Otros sistemas locales/departamentales: sus responsables y administradores

Como ya se ha expuesto anteriormente, pueden existir recursos que presten servicio a un Centro, Instituto Unidad Asociada o a un grupo concreto de usuarios del CSIC. Estos recursos tendrán también un Responsable Administrativo y un administrador del sistema, distintos del CTI, y cuyo ámbito de actuación se reduce a los recursos bajo su responsabilidad.
Aparte de todas las actividades relacionadas en el punto anterior, el administrador del sistema debe procurar:
- Implantar y hacer cumplir en su ámbito de actuación la política y normas generales, así como las particulares de ámbito.
- Coordinarse y colaborar con el CTI en el uso de los recursos globales.
- Mantener actualizados y seguros los sistemas bajo su responsabilidad.

Será el Responsable Administrativo quien deba responder ante incidencias e incumplimiento de la política por parte del sistema local.

### 5.3. El Responsable de Seguridad.

De entre el personal del CSIC, y destinado en el CTI, se nombrará una persona, unidad organizativa u órgano colegiado, denominada Responsable de

Seguridad, que será quien se debe encargar de dirigir las medidas y acciones para hacer cumplir esta política, así como de su interpretación, control de cumplimiento y resolución de los problemas relativos a la misma:

- Interpretación de la política: Será responsable de la interpretación de esta política, de la resolución de los problemas y conflictos con las políticas locales o departamentales y otras situaciones especiales.
- Cumplimiento de la política: en los casos en que incurran violaciones a esta política, el Responsable de seguridad estará autorizado a trabajar en colaboración con las correspondientes unidades administrativas para su resolución.
- Control y monitorización: será el responsable de diseñar la arquitectura y medidas de seguridad, la implantación de herramientas y técnicas y su grado de cumplimiento y ajuste a esta política.

Asumirá también todas las funciones y responsabilidades definidas en el Reglamento de medidas de seguridad para ficheros con datos de carácter personal (Real Decreto 994/1999) para Responsables de seguridad. Para asuntos legales derivados del incumplimiento de estas normas se consultará con la Asesoría Jurídica.

## 6. LAS CONSECUENCIAS DEL MAL USO DE LOS RECURSOS:

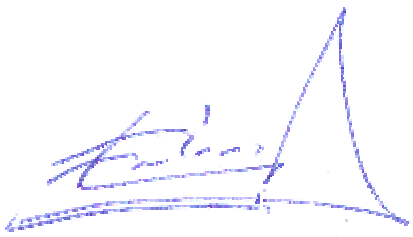
**6.1. Colaboración de los usuarios:** los usuarios, cuando se les solicite, deben colaborar con los administradores de sistemas, en la medida de sus posibilidades, en cualquier investigación que se haga sobre mal uso de los recursos, aportando la información que se les requiera.

**6.2. Acciones correctivas y preventivas:** si los administradores del sistema (generales o locales) 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 a los superiores u órganos de gobierno correspondientes de lo sucedido.

**6.3. 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 Responsable de seguridad.

En Madrid a diecinueve de febrero de dos mil cuatro.



Eusebio Jiménez Arroyo
Secretario General