INSTRUCCIÓN DE 21 DE MAYO DE 2019, de la Secretaría General del Consejo Superior de Investigaciones Científicas, por la que se aprueba la Norma General de Seguridad Informática para la utilización de los recursos y sistemas corporativos de información del Consejo.

El acceso a las redes de comunicaciones, la utilización de equipamiento informático, servicios de red y sistemas de información son actualmente una necesidad de cualquier organización y, en concreto, del Consejo Superior de Investigaciones Científicas (en adelante CSIC). Los medios y recursos se ponen a disposición de los usuarios como instrumentos de trabajo para el desempeño de su actividad profesional, razón por la que compete y es obligación del CSIC determinar las normas, condiciones y responsabilidades bajo las que se deben utilizar tales recursos tecnológicos.

La Agencia Estatal CSIC aprobó, mediante Resolución de la Presidencia del 8 de julio de 2014, la Política de Seguridad de la Información del Organismo. Esta Política de Seguridad determina, en su apartado tercero "Desarrollo normativo de la Política de Seguridad de la Información", los distintos niveles que compondrán el cuerpo normativo de Seguridad de la Información del CSIC.

En el primer nivel normativo se encuadra la mencionada Política de Seguridad de la Información del CSIC, así como la Instrucción de 9 de julio de 2014, de la Secretaría General del CSIC, por la que se desarrolla la estructura organizativa de la seguridad de la información. El segundo nivel corresponde a las Normas de Seguridad (instrucciones o circulares) específicas, mediante las que se desarrollará la Política de Seguridad y en las que se han de regular áreas o aspectos relevantes de aplicación en toda la organización. La norma establece, por último, un tercer nivel –denominado Procedimientos de Seguridad– que está compuesto por procedimientos y guías que detallan instrucciones de carácter técnico o procedimental.

La presente Instrucción, dictada por el Secretario General en calidad de Presidente del Comité Corporativo de Seguridad de la Información, contiene el desarrollo normativo de segundo nivel de seguridad de la información en el CSIC. Consta de un cuerpo central, que incluye el marco general que conforma la Norma de Seguridad Informática del CSIC, y de un conjunto de Anexos, con el desarrollo de Normas de carácter específico sobre determinados ámbitos.

Esta normativa de Seguridad Informática complementa la aplicación de las medidas de seguridad previstas en el Anexo II del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica (ENS).

PRIMERO.- DISPOSICIONES GENERALES.

1.1 OBJETO

Esta Norma General de Seguridad Informática tiene por objeto establecer las disposiciones encaminadas a alcanzar la mayor eficacia y seguridad en el uso de los recursos y de la información en el CSIC, basándose para ello en los principios de disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad.

Los Institutos, Centros y Unidades (ICU) del CSIC podrán ampliar la normativa de Seguridad Informática del CSIC, desarrollando normas de carácter interno que deberán ser complementarias, congruentes y no

entrar en conflicto con esta Norma. Corresponde a los directores de los ICU la aprobación de tales normas complementarias, y las Gerencias y órganos asimilados de los ICU serán los encargados de su difusión en su ámbito de responsabilidad, así como del control de su cumplimiento, incluido el cumplimiento de la presente Instrucción Operativa.

Todas las disposiciones que componen la normativa de Seguridad Informática del CSIC, junto con las que puedan incorporarse en el futuro, son documentos de carácter y uso interno del CSIC.

1.2 ÁMBITO DE APLICACIÓN

Esta Instrucción se aplicará a todo el personal que forma parte, colabora o está vinculado con el CSIC, en todo lo relativo al acceso y uso que haga de datos, recursos y medios, infraestructuras e instalaciones, servicios, sistemas de información o cualquier otro medio para el acceso y tratamiento de la información que sean propiedad del CSIC. Asimismo, se aplicará a cualquier persona física o jurídica que haga uso o tenga acceso a éstos.

En el ámbito de esta Instrucción, se entiende por "usuario" cualquier persona que tenga acceso a la información, sistemas y/o recursos TIC del CSIC con independencia del tipo de vinculación que pudiera mantener con esta Agencia Estatal.

SEGUNDO.- COMPETENCIAS Y FUNCIONES.

2.1. ROLES Y FUNCIONES

A lo largo de esta Norma se hace referencia y se concretan los roles y funciones definidos en la Instrucción de 9 de julio de 2014, de la Secretaría General del CSIC, por la que se desarrolla la estructura organizativa de la seguridad de la información, de acuerdo con las funciones y responsabilidades que correspondan en cada caso y que deben entenderse conforme allí aparecen definidos.

Se describen, a continuación, los roles y funciones relativos al Grupo Técnico de Seguridad, como principal agente en la construcción de la normativa general de seguridad en materia TIC en el CSIC y los correspondientes a los agentes directamente implicados en el diseño y ejecución de la función TIC en la institución.

El Grupo Técnico de Seguridad de la Información

El Grupo Técnico de Seguridad de la Información del CSIC es el órgano competente para propiciar, dirigir y supervisar el adecuado cumplimiento de esta Instrucción, para lo que ejerce las siguientes funciones con apoyo de la SGAI:

- Coordinar las actuaciones derivadas de la aplicación de la Norma de Seguridad Informática del CSIC.
- Interpretar las dudas que puedan surgir en su aplicación.

- Proceder a la revisión de las disposiciones que componen la Norma de Seguridad Informática del CSIC, ya sea de oficio o ante una petición formalmente presentada y, si procede, redactar una propuesta de nueva versión que deberá ser sometida a la aprobación del Comité Corporativo de Seguridad Informática del CSIC. La revisión de la normativa se llevará a cabo como mínimo una vez al año. La revisión se orientará tanto a la identificación de oportunidades de mejora en la gestión de la seguridad de la información como a su adaptación ante cambios organizativos, en el marco legal, infraestructuras tecnológicas o de cualquier otra índole que lo justifique.
- Verificar su efectividad.

La Función TIC en el CSIC

En el marco de la presente Norma, Función TIC engloba a todos aquellos trabajos cuya actividad principal se centra en los ámbitos de la gestión, administración y configuración de equipamiento informático (equipos de usuario, servidores, almacenamiento e infraestructura de sistemas en general), equipamiento de comunicaciones (routers, conmutadores, gateways y centralitas, entre otros), equipamiento de seguridad (cortafuegos, IPS, IDS, analizadores de vulnerabilidades, analizadores de flujo, sondas, etc.), así como actividades estrechamente ligadas con el desarrollo de aplicaciones informáticas, generalmente de carácter corporativo.

Todo lo anterior se debe entender como el ejercicio de tareas orientadas o bien a prestar un servicio horizontal, sea para el CSIC y todo su personal de forma global o sea para un ICU y el personal adscrito al mismo, o bien a prestar un servicio a grupos o colectivos específicos, como ocurre con el personal que presta servicios informáticos a uno o varios grupos de investigación.

A lo largo de la presente normativa se hará referencia a la Función TIC de formas diversas, tales como "tareas TIC", "servicios informáticos", "servicios TIC", etc., siendo prestados por alguno de los agentes de la Función TIC definidos a continuación.

Los agentes de la Función TIC en el CSIC

La singularidad de la misión y estructura organizativa del CSIC tiene efectos sobre la diversidad de la función TIC y destinatarios de la misma en la Institución.

En base a los destinatarios de los servicios, se pueden diferenciar los siguientes tipos de rol TIC en el CSIC:

- **TIC-Horizontal**: Este rol está orientado a personal que presta mayoritariamente servicios de carácter horizontal y general en materia TIC en el CSIC, ya estén dirigidos a su unidad de adscripción (ICU) o a toda la institución.
- **TIC-Proyectos**: En este rol se encuadra el personal que ofrece principalmente servicios TIC destinados a grupos o colectivos determinados, principalmente grupos de investigación, y generalmente dentro del marco de desarrollo y ejecución de proyectos de investigación.

Los agentes de la Función TIC, a lo largo de la presente Norma, podrán ser aludidos de diversas formas, tales como "personal TIC", "personal informático", u otros de naturaleza análoga.

La normativa aprobada mediante esta Instrucción tiene carácter universal en el ámbito del CSIC.

De forma particular, todo el personal TIC, con independencia de su rol específico, ha de respetar y cumplir la presente Norma en todo aquello que haga referencia expresa a funciones, responsabilidades y tareas específicas del "personal TIC".

2.2 PERSONAL AUTORIZADO PARA TAREAS TIC

El personal TIC de la Organización Central (ORGC), como norma general, tendrá dependencia orgánica y funcional de la Secretaría General Adjunta de Informática (SGAI), y será el único que podrá realizar las tareas de mantenimiento, desarrollo, gestión, administración y soporte de los servicios y sistemas, así como del parque de equipos e infraestructuras TIC destinado tanto a ofrecer los servicios corporativos como aquellos propios de la ORGC del CSIC.

Con carácter excepcional, determinadas unidades de la ORGC distintas de la SGAI podrán contar con personal TIC que preste exclusivamente servicios informáticos específicos de apoyo a la propia unidad para el adecuado desempeño de sus funciones, y nunca de carácter horizontal. En todo caso, su desempeño profesional podrá ser supervisado, y modificado conforme a las directrices funcionales de la SGAI.

Como norma general, todo el personal que preste servicios TIC de carácter horizontal en los ICU tendrá dependencia orgánica y funcional de la Gerencia del ICU, aunque en condiciones excepcionales su desempeño profesional, principalmente en materia de seguridad, podrá ser supervisado y modificado conforme a las directrices funcionales de la SGAI.

En el caso del personal que desarrolle actividades TIC fundamentalmente para grupos de investigación, unidades de servicio u otros departamentos o colectivos específicos (rol TIC-P), su actividad dependerá del responsable del grupo en el que participa; o de la jefatura del departamento, Dirección o Vicedirección cuando sus servicios se ofrecen a distintos grupos o unidades. En todo caso, sus actuaciones quedarán supeditadas y no podrán contravenir las normas de seguridad informática implantadas en el ICU. Para el adecuado desenvolvimiento de los servicios y sistemas informáticos corporativos en los ICU es imprescindible la coordinación de actuaciones y eficaz colaboración de las unidades de servicios TIC de los ICU y de la ORGC; siendo preciso para ello conocer la identidad de los Responsables y del resto de Personal TIC de los ICU. Por las razones mencionadas, la Dirección, Vicedirección, Gerencia u órgano asimilado deberá comunicar a la SGAI las altas y las bajas y, en general, cualquier cambio que suponga una variación en las personas o funciones TIC asignadas, siempre con anterioridad o simultaneidad al inicio del desempeño o cese de la actividad.

2.3 CUMPLIMIENTO Y SUPERVISIÓN DE ESTA NORMATIVA.

La SGAI, cumpliendo en todo momento los requisitos que al efecto establece la legislación vigente, en el marco de sus competencias y particularmente en su función de apoyo al Grupo Técnico de Seguridad Informática para propiciar, dirigir y supervisar el adecuado cumplimiento de la Norma General de Seguridad Informática y las Normas específicas que se aprueben en desarrollo y ejecución de esta Instrucción, tendrá potestad para llevar a cabo las siguientes actuaciones en todo el CSIC:

- Revisar periódicamente el estado de los equipos, el software instalado, los dispositivos y redes de comunicaciones.

- Monitorizar los accesos a la información contenida en los sistemas que gestiona y administra.
- Auditar la seguridad de las credenciales y aplicaciones, y definir mecanismos que garanticen unos niveles mínimos de robustez en el acceso y uso de los sistemas y servicios que gestiona y administra.
- Monitorizar los servicios de Internet, servicios en red y otras aplicaciones mediante el empleo de los dispositivos y sistemas de seguridad con los que cuente el CSIC en cada momento.
- Realizar auditorías sobre el estado de la red de comunicaciones y sobre su seguridad y de los recursos conectados a ella.

Esta actividad de monitorización será llevada a cabo sin utilizar sistemas o programas que pudieran atentar contra los derechos fundamentales de los usuarios, tales como el derecho a la intimidad personal y al secreto de las comunicaciones, manteniéndose en todo momento la privacidad de la información manejada, salvo que, por requerimiento judicial o investigación sobre un uso ilegítimo o ilegal fundamentada y autorizada expresamente por el Comité Corporativo de Seguridad de la Información, sea necesario el acceso a dicha información.

Los sistemas o equipos en los que se detecte un uso inadecuado, ilegítimo o ilegal, cuya seguridad haya sido vulnerada o en los que no se cumplan los requisitos mínimos de seguridad informática, podrán ser bloqueados o suspendidos temporalmente por la SGAI, previa decisión del Comité Corporativo de Seguridad de la Información. El servicio se restablecerá cuando la causa de su vulnerabilidad o degradación desaparezca a juicio de la SGAI.

Asimismo, por estrictas razones de seguridad, se podrá limitar o bloquear el acceso a determinadas páginas web o servicios informáticos, así como retener mensajes de correo electrónico con contenido sospechoso o peligroso, mediante el uso automatizado de filtros con listados de sitios y tipologías de mensajes potencialmente peligrosos o inadecuados, sin perjuicio de las trazas y los registros obtenidos por los sistemas de monitorización y control implantados (duración de las conexiones, volumen de datos intercambiado, etc.). Esta actuación se llevará a cabo por la SGAI, dando cuenta inmediatamente al Comité Corporativo de Seguridad de la Información, que podrá mantener o revocar la limitación o bloqueo.

Normativas específicas y control de versiones.

El Grupo Técnico de Seguridad de la Información, cuando concurran circunstancias que lo justifiquen, actualizará aquellas normativas específicas que lo requieran, procediendo a elaborar una nueva versión actualizada de las mismas, a la que se le dará la adecuada difusión.

De igual forma, se mantendrá publicada en la intranet del CSIC la última versión vigente de cada normativa específica, con indicación de la versión correspondiente de la misma y de la fecha de su entrada en vigor.

El Grupo Técnico de Seguridad de la Información, conforme a las funciones y responsabilidades encomendadas y recogidas en la Instrucción de 9 de julio de 2014 de la Secretaría General del CSIC, diseñará e implantará los controles de seguridad necesarios para verificar el cumplimiento de la presente Normativa General y dará cuenta al Comité Corporativo de Seguridad de la Información acerca de las actividades llevadas a cabo, así como sobre las deficiencias de seguridad informática observadas y los posibles incumplimientos de la presente normativa, al objeto de que se tomen las medidas oportunas.

En el supuesto de que un usuario no observe alguno de los preceptos señalados en la presente Normativa General, en sus Normas Específicas o en las guías o procedimientos de desarrollo, sin perjuicio de las acciones disciplinarias y administrativas que procedan de acuerdo con el Real Decreto 5/2015, de 30 de octubre, por el que se aprueba el Texto Refundido del Estatuto del Empleado Público y su normativa de desarrollo y, en su caso, las responsabilidades legales correspondientes, se podrá acordar por el Comité Corporativo de Seguridad de la Información la suspensión temporal o definitiva del uso de los recursos informáticos que tenga asignados, y por la SGAI con carácter preventivo.

DISPOSICIÓN FINAL PRIMERA.- DESARROLLO NORMATIVO E INTERPRETACIÓN.

Se autoriza a la SGAI para que dicte cuantas circulares sean necesarias para el desarrollo y ejecución de lo previsto en esta Instrucción y al Responsable de Seguridad para que publique las guías y estándares que implementen lo establecido en el cuerpo normativo de seguridad, de acuerdo con la Instrucción de 9 de julio de 2014 de la Secretaría General del CSIC. Igualmente, la SGAI, en su función de apoyo al Grupo Técnico de Seguridad de la Información, se encargará de interpretar cuantas dudas puedan producirse en la aplicación de la presente Instrucción.

En todo caso, la SGAI deberá aprobar la normativa específica que corresponda, al menos, sobre los siguientes dominios y materias:

1. Dominio de Comunicaciones
    a. Seguridad para el acceso a Internet.
    b. Seguridad para la conexión de dispositivos a las redes de comunicaciones.
2. Dominio de Sistemas, equipamiento e infraestructuras
    a. Seguridad para el uso de equipos de trabajo y servidores.
    b. Seguridad para el mantenimiento de equipamiento hardware y software.
    c. Seguridad para las copias de respaldo (backups).
    d. Seguridad para el uso de impresoras de red, fotocopiadoras, escáneres, faxes y equipos multifunción.
3. Dominio de Desarrollo
    a. Autenticación y Firma. Gestión de permisos y roles.
    b. Seguridad para el uso de la información.
    c. Seguridad para el desarrollo de aplicaciones y sitios web.
    d. Seguridad para la protección de los datos de carácter personal.
4. Dominio de Seguridad física
    a. Seguridad en Centros de Proceso de Datos (CPDs) y salas técnicas

DISPOSICIÓN FINAL SEGUNDA.- ENTRADA EN VIGOR.

Esta Instrucción entrará en vigor al día siguiente de su publicación en BO.CSIC.

Firmado electrónicamente por el Secretario General del CSIC,

Alberto Sereno Álvarez