INSTRUCCIÓN DE 8 DE MAYO DE 2024, de la Secretaría General del Consejo Superior de Investigaciones Científicas, por la que se modifican las Instrucciones de 9 de julio de 2014 y de 15 de junio de 2019, por las que se desarrolla y modifica, respectivamente, la estructura organizativa de la seguridad de la información en la Agencia Estatal CSIC.

Con fecha 9 de julio de 2014, la Secretaría General del CSIC aprobó la Instrucción de desarrollo de la estructura organizativa de la seguridad de la información de la Agencia Estatal CSIC. Esta instrucción desarrolla determinados aspectos de la Resolución de 8 de julio de 2014 de la Presidencia del CSIC, por la que se aprueba la Política de la Seguridad de la Información del CSIC. El objetivo de esta Resolución es contribuir a la creación de las condiciones necesarias de confianza en el uso de medios electrónicos a través de medidas que permitan garantizar la seguridad de los sistemas, los datos, las comunicaciones y los servicios electrónicos, permitiendo a los ciudadanos y administraciones públicas el ejercicio de derechos y el cumplimiento de obligaciones por estos medios, en el marco de lo establecido por la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos y el Real Decreto 3/2010, de 8 de enero, que regula el Esquema Nacional de Seguridad.

Dentro de este marco, los aspectos que regula la Instrucción de 9 de julio de 2014 se centran en el desarrollo pormenorizado de la estructura organizativa y de los agentes encargados de la ejecución de esta política en la Agencia Estatal CSIC, de acuerdo con las previsiones recogidas en la Resolución de 8 de julio de 2014.

La aprobación de Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público así como del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, que deroga el Real Decreto 3/2010 mencionado previamente, así como la aprobación del Contrato de Gestión del CSIC, conllevan la necesidad de actualizar determinados preceptos de la estructura organizativa de la Agencia Estatal CSIC para dotarlo de la necesaria amplitud y flexibilidad que permita dar cabida a la variedad de centros e institutos de investigación con que cuenta la Agencia Estatal CSIC y sus respectivas realidades, y permita conformar un marco de gobernanza de la seguridad efectivo, ágil y adecuado a la realidad del Consejo.

Esta Secretaría General, en uso de las atribuciones que tiene conferidas en el artículo 19.l.b) y e) del Estatuto de la Agencia Estatal CSIC, aprobado por Real Decreto 1730/2007, de 21 de diciembre, dispone la modificación en la regulación de la estructura organizativa de la política de seguridad de la información del CSIC, en los siguientes términos:

PRIMERO.- MODIFICACIÓN DE LAS INSTRUCCIONES DE 9 DE JULIO DE 2014 Y DE 15 DE JUNIO DE 2019, DE LA SECRETARÍA GENERAL DEL CSIC, POR LAS QUE SE DESARROLLA Y MODIFICA, RESPECTIVAMENTE, LA ESTRUCTURA ORGANIZATIVA DE LA SEGURIDAD DE LA INFORMACIÓN EN LA AGENCIA ESTATAL CSIC.

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 en la Agencia Estatal CSIC, se modifica en los siguientes términos:

Uno. El apartado "SEGUNDO.- Estructura organizativa" queda redactado del siguiente modo:

La estructura organizativa de la seguridad en la Agencia Estatal CSIC deberá contemplar las especificidades inherentes a la realidad de la estructura administrativa del organismo. Por ello, se tendrán en cuenta tanto aspectos generales y globales, como particularidades específicas de los Institutos, Centros y Unidades, con el fin de que todos ellos puedan tener el adecuado encaje en lo relativo a la estructura organizativa en materia de seguridad de la información.

Con carácter general, se contemplan 4 niveles o ámbitos de actuación en materia de seguridad de la información:

- Nivel de gobierno
- Nivel de supervisión
- Nivel de especificación
- Nivel de operación

Podrán estar compuestos tanto por los correspondientes comités como por perfiles profesionales determinados, no siendo necesario que en todos los niveles existan comités específicos.

2.1 LOS COMITÉS DE SEGURIDAD DE LA INFORMACIÓN.

2.1.1 Nivel de gobierno. El Comité Corporativo de Seguridad de la Información.

El *Comité Corporativo de Seguridad de la Información* es el órgano decisorio encargado de mantener actualizada y adaptada la Política de Seguridad de la Información en el CSIC y de velar por su cumplimiento, para lo que deberá coordinar a las distintas áreas y unidades que intervienen en esta materia y promover la difusión del contenido de la política entre el personal de la Institución.

Asimismo, se encargará de establecer y mantener actualizados los criterios y directrices generales sobre seguridad de la información, del seguimiento y control de los objetivos del Contrato de Gestión del CSIC en lo que afecta a cuestiones de seguridad y de acordar y hacer operativas medidas para mejorar y reforzar los sistemas de seguridad y control.

Estará formado por el titular de la Secretaría General del CSIC, que actuará como Presidente, y los titulares o representantes designados de las Secretarías Generales Adjuntas de Informática y de Recursos Humanos, de la Asesoría Jurídica y de la Oficialía Mayor. El Comité contará con un Secretario, que será el Responsable de Seguridad en el CSIC.

Con carácter excepcional, la persona que ocupe la Presidencia podrá solicitar la presencia de los titulares, o representantes designados, de cualquiera de las Vicepresidencias del CSIC u otros órganos directivos en las reuniones del Comité, cuando por razón de los asuntos a tratar lo considere necesario.

El *Comité Corporativo de Seguridad* deberá dar cuenta de su gestión a la Presidencia a través de la Secretaría General.

El *Comité Corporativo de Seguridad* podrá reunirse con carácter ordinario y extraordinario, pudiendo adoptar en reunión virtual sus decisiones, utilizando los medios electrónicos disponibles.

Se reunirá con carácter ordinario al menos una vez al año previa convocatoria de su Presidente.

El Comité se podrá reunir con carácter extraordinario cuantas veces considere necesario su Presidente, siempre que se produzcan incidencias graves que pudieran afectar a la seguridad de la información y de los sistemas corporativos que la gestionan o existan necesidades de seguridad que requieran la coordinación de las áreas en que se estructura la Organización Central. El Presidente reunirá con carácter extraordinario a todos o a parte de los miembros del Comité en función de las necesidades de los asuntos a tratar.

Para cumplir con sus fines el Comité deberá desarrollar las siguientes funciones:

a) Elaborar las propuestas de modificación y actualización permanente de la Política de Seguridad de la Información del CSIC.

b) Velar por el cumplimiento de la normativa que resulte de aplicación.

c) Coordinar las funciones de seguridad de la información del CSIC al máximo nivel.

d) Recabar informes periódicos del estado de la seguridad de la información del CSIC y de los incidentes registrados procedentes de la Oficina Técnica de Seguridad.

2.1.2 Nivel de supervisión. La Oficina Técnica de Seguridad de la Información.

Mediante Instrucción de la Secretaría General del CSIC se constituirá la O*ficina Técnica de Seguridad de la Información del CSIC* (en adelante, OTS), como órgano de apoyo y asesoramiento al *Comité Corporativo de Seguridad de la Información*, así como para la coordinación y supervisión de la seguridad implantada por los distintos centros e institutos de investigación y por las unidades de la Organización Central con responsabilidades en la gestión y administración de infraestructuras TIC.

Esta *Oficina Técnica de Seguridad* tiene por objeto realizar propuestas normativas, diseñar acciones para su puesta en marcha, así como velar por la mejora continua de la seguridad de la información, tanto a nivel de la Organización Central como de los Centros e Institutos, siendo el nexo de unión entre el Comité Corporativo de Seguridad de la Información y los Comités de Seguridad de los Centros e Institutos, supervisando la correcta implantación de la seguridad en estos últimos.

La persona que ostente en el CSIC el rol de *Responsable de Seguridad de la Información* definido en el Esquema Nacional de Seguridad actuará como Director de la OTS, siendo en particular responsable del nombramiento de los demás integrantes de la OTS, que conformarán un Gabinete de *Responsables de Seguridad Delegados*.

La OTS podrá contar con la participación del *Delegado de Protección de Datos* en aquellas cuestiones de Seguridad vinculadas al tratamiento de datos de carácter personal.

Sin perjuicio de lo anterior, la Instrucción de creación de la *Oficina Técnica de Seguridad de la Información* recogerá los detalles oportunos tanto de su composición y estructura como de sus responsabilidades y funciones.

2.1.3 Nivel de especificación. Los Comités de Seguridad de Centros, Institutos y Unidades.

Cada ICU contará con un *Comité de Seguridad* en el ámbito del propio Centro, Instituto o Unidad, que será el órgano decisorio encargado de coordinar la aplicación de las políticas y normas de seguridad corporativas en el ámbito del ICU, para lo que deberá coordinar a las distintas unidades que intervienen en la materia en el ámbito de responsabilidad del propio ICU.

Se encargará de dar traslado a la *Oficina Técnica de Seguridad de la Información* del análisis y evaluación de los riesgos realizado por los *Responsables del Sistema* del ICU, en coordinación con los *Responsables de la Información* y *Responsables del Servicio*, así como de establecer y mantener actualizados los criterios y directrices específicos sobre seguridad de la información en el ámbito del ICU, complementariamente a todos aquellos de carácter corporativo y general establecidos desde la Organización Central o desde entidades externas con responsabilidad superior en materia de seguridad y de acordar y hacer operativas medidas para mejorar y reforzar los sistemas de seguridad y control.

El rol de *Responsable/s del Sistema* en el ICU podrá recaer en el responsable de la agrupación que preste servicio al ICU o en personal TIC de apoyo y respaldo que administre infraestructuras y recursos pertenecientes a dicho ICU. Estarán adscritos a la División a la que funcionalmente corresponda el recurso a administrar y securizar.

De forma transitoria, hasta la completa implantación del nuevo modelo de gobernanza TIC, el rol de *Responsable del Sistema* por defecto será asumido por la persona que ejerza las funciones de *responsable TIC del ICU.*

El Comité estará formado por las personas que ocupan los cargos de Dirección del ICU, Gerencia del ICU, los Jefes de Unidad o Departamento del ICU (o un subconjunto de los mismos, en función de la dimensión del ICU) y el *Responsable de la Agrupación* que da servicio al ICU, o bien la *persona TIC de apoyo* en

quien el *Responsable de la Agrupación* delegue. Deberá dejarse constancia escrita de la composición del Comité en cada ICU, tanto en su constitución inicial como en las posibles modificaciones posteriores, debiendo remitirse copia del acta de dicha composición a la Oficina Técnica de Seguridad de la Información.

Dicha composición podrá ser adaptada y particularizada para hacerla compatible con las modificaciones estructurales que se puedan producir a nivel organizativo y operativo tanto en el ámbito de funciones y responsabilidades gerenciales como en el de prestación de servicios TIC, tratando de preservar los principios de cercanía y mejor conocimiento de las infraestructuras, recursos y funcionamiento interno del ICU y aprovecharlos en beneficio de la seguridad.

El Comité contará con un Secretario, que será la persona que ocupe el cargo de Gerencia del ICU o desempeñe funciones equivalentes, en base a las posibles modificaciones organizativas y operativas referidas en el párrafo anterior.

El *Comité de Seguridad del Centro o Instituto* deberá dar cuenta de su gestión al *Comité Corporativo de Seguridad de la Información* a través de la *Oficina Técnica de Seguridad de la Información*.

El *Comité de Seguridad del Centro o Instituto* podrá reunirse con carácter ordinario y extraordinario, pudiendo adoptar en reunión virtual sus decisiones, utilizando los medios electrónicos disponibles.

Se reunirá con carácter ordinario al menos una vez al año.

El Comité se podrá reunir con carácter extraordinario cuantas veces considere necesario cualquiera de sus miembros, siempre que se produzcan incidencias graves que pudieran afectar a la seguridad de la información en el ICU o existan necesidades de seguridad que lo justifiquen. Se podrán reunir con carácter extraordinario todos o una parte de los miembros del Comité, en función de las necesidades de los asuntos a tratar.

Para cumplir con sus fines el Comité deberá desarrollar las siguientes funciones:

a) Velar por el cumplimiento de la normativa que resulte de aplicación, tanto general como específica del ICU.

b) En caso de considerarlo oportuno, elaborar y aprobar normas específicas de seguridad en el ámbito del ICU, siempre que no entren en conflicto con las políticas y normas de seguridad de carácter corporativo y general.

c) Coordinar las funciones de seguridad de la información en el ámbito del ICU.

d) Recabar informes periódicos del estado de la seguridad de la información en el ámbito del ICU y de los incidentes registrados y remitirlos a la *Oficina Técnica de Seguridad de la Información*.

e) Coordinar los planes de continuidad de las distintas unidades del ICU para garantizar una actuación coordinada y sin fisuras en caso de que deban activarse.

f) Fomentar la cultura de la seguridad de la información en el ámbito del ICU, complementariamente a las iniciativas de carácter general que puedan llevarse a cabo en todo el CSIC.

Sin perjuicio de lo anterior, de forma específica por sus especiales condiciones y características, en el Anexo A se detalla la Organización de la Seguridad en la Organización Central del CSIC, así como las particularidades que conciernen a la Secretaría General Adjunta de Informática.

2.2 Los Grupos de Trabajo de Seguridad de la Información.

Dada la dimensión de la Institución, su dispersión geográfica, su complejidad organizativa y funcional y la multiplicidad cuantitativa y cualitativa de sus necesidades en materia de seguridad de la información, se podrán crear Grupos de Trabajo de Seguridad de la Información de forma complementaria e independiente de los comités definidos en el apartado anterior.

Estos Grupos de Trabajo tendrán por objeto el análisis de las necesidades de seguridad TIC sobre una materia concreta, la valoración técnica de alternativas, así como la elaboración y presentación de propuestas a la Oficina Técnica de Seguridad de la Información.

La solicitud de creación de un Grupo de Trabajo tendrá lugar, de forma motivada, a iniciativa del *Responsable de Seguridad* del CSIC, de alguno de los responsables de las divisiones o áreas funcionales o bien de alguno de los coordinadores de un *Centro de Gestión de Servicios TIC* (CGSTIC) o responsables de alguna de las agrupaciones adscritas a los mismos, en función de la naturaleza, finalidad y ámbito perseguidos por dicho Grupo de Trabajo. La creación deberá de ser comunicada al *Responsable de Seguridad de la Información,* indicando la finalidad del Grupo de Trabajo y los miembros que lo componen inicialmente.

2.3 LOS AGENTES RESPONSABLES EN LA SEGURIDAD DE LA INFORMACIÓN: PERFILES PROFESIONALES.

Los responsables en materia de seguridad de la información son los agentes encargados de la implantación y ejecución, seguimiento y control de las normas y procedimientos aprobados por los comités de seguridad.

Tales agentes, que actuarán de acuerdo a los niveles de servicio, dispondrán de los perfiles profesionales que se recogen a continuación y ejercerán las siguientes funciones:

2.3.1 Nivel de supervisión.

a) Responsable de la Seguridad.

El perfil de *Responsable de Seguridad* tiene por objeto mantener la seguridad de la información y de los servicios ofrecidos por los sistemas de información en su ámbito de responsabilidad.

A tal fin será nombrado por el *Comité Corporativo de Seguridad* por períodos de dos años renovables por el mismo período.

El *Responsable de Seguridad de la Información* ejercerá las siguientes funciones:

a) Elaborar una planificación estratégica de la seguridad de la información del CSIC a largo plazo, considerando la misión y objetivos de la Organización, así como la evolución de la tecnología y las responsabilidades legales.

b) Promover la formación y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad.

c) Determinar los niveles de seguridad de la información requeridos en cada dimensión.

d) Determinar la categoría de los sistemas, a partir de la valoración y propuesta efectuada de forma coordinada entre los *Responsables de la Información*, *de los Servicios* y *del Sistema*.

e) Aprobar los diferentes análisis de riesgos recibidos, revisados y validados por la Oficina Técnica de Seguridad de la Información.

f) Informar sobre el estado de la seguridad del sistema que monitorizarán los *Administradores de la Seguridad de los Sistemas*.

g) Revisar y en su caso validar, los planes de continuidad elaborados por los Responsables correspondientes respecto de los recursos e infraestructuras administrados en sus respectivos ámbitos de responsabilidad.

El *Responsable de la Seguridad* podrá designar *Responsables de Seguridad Delegados* que colaborarán con él y le prestarán apoyo para el mejor desempeño de su actividad. A través de esta designación el *Responsable de la Seguridad* podrá delegar funciones en los *Responsables de Seguridad Delegados*, si bien la responsabilidad final seguirá recayendo sobre el *Responsable de Seguridad*. El gabinete de *Responsables de Seguridad Delegados*, junto con el propio *Responsable de Seguridad*, conformarán la *Oficina Técnica de Seguridad de la Información* del CSIC. En caso necesario podrán contar con personal externo de apoyo para la ejecución de sus funciones

Por su parte, los delegados deberán acometer las tareas que les hayan sido asignadas, debiendo informar y dar cuenta de sus actuaciones al *Responsable de Seguridad*.

2.3.2 Nivel de especificación.

En el nivel de especificación se incluyenlos roles de *Responsable de la Información* y *Responsable del Servicio* definidos por el Esquema Nacional de Seguridad.

La naturaleza de las responsabilidades inherentes a cada unidad del CSIC y los procedimientos gestionados por la misma, y su traslación al correspondiente sistema de información se traducirán en muchas ocasiones en una coincidencia de ambas responsabilidades (de la información y del servicio) en una misma

persona o unidad, siendo de aplicación los preceptos, responsabilidades y actuaciones a desarrollar de forma común desde la perspectiva de ambos roles.

En determinados casos podrá darse una separación y diferenciación de responsabilidades entre un determinado servicio y la información gestionada por el mismo, por corresponder a diferentes unidades en base a condicionantes específicos de cada caso particular.

Sin perjuicio de lo anterior, en aquellos servicios que gestionen información que contenga datos de carácter personal, serán de aplicación el Reglamento General de Protección de Datos y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, y en particular deberá contemplarse el rol de *Responsable del Tratamiento*.

a) Responsable de la Información y del Servicio.

En aquellos casos en los que las responsabilidades de la información y del servicio confluyan en una misma unidad, persona u órgano, estas se unificarán en el *Responsable de la Información y del Servicio*, siendo de aplicación lo estipulado en el presente apartado.

El *Responsable de la Información y del Servicio* será el encargado de controlar la utilización de una determinada información en el contexto del servicio o servicios que la gestionan.

En la Organización Central esta responsabilidad recaerá sobre el titular del órgano o unidad administrativa que gestione cada procedimiento administrativo o sea responsable funcional de cada aplicación corporativa, pudiendo una misma persona acumular las responsabilidades de la información y de los servicios asociados a todos los procedimientos o aplicaciones que gestione.

En el caso de Institutos o Centros, esta responsabilidad recae sobre el Gerente en los temas de carácter horizontal; tendrán asimismo la condición de *Responsables de la Información y de los Servicios* los titulares o responsables de las unidades o grupos de investigación respecto a la información que generen o gestionen, particularmente en caso de proyectos de investigación.

La responsabilidad de la información y del servicio podrá recaer en un conjunto de personas constituidas colegiadamente como comité o grupo de trabajo, el cual podrá formar parte de, o estar integrado en, el *Comité de Seguridad del Centro o Instituto*.

El *Responsable de la Información y del Servicio* asumirá la responsabilidad última del uso que se haga de la información que le compete y del servicio asociado que la gestiona, así como de su protección, debiendo por tanto preservar su integridad y su carácter de confidencialidad.

El *Responsable de la Información y del Servicio* ejercerá la potestad de determinar los niveles de seguridad aplicables a la información y al servicio asociado, que serán alto, medio o bajo, para cada una de las cinco dimensiones de la seguridad: disponibilidad (del servicio), y autenticidad, integridad, confidencialidad y trazabilidad (de la información).

En la determinación de los niveles de seguridad por el *Responsable de la Información y del Servici*, es recomendable que éste recabe asesoramiento del *Responsable del Sistema* y también, en su caso, de la Oficina Técnica de Seguridad . En caso de discrepancia de criterios y ante la ausencia de superior jerárquico común, cualquiera de los perfiles señalados podrá elevar una consulta al *Comité Corporativo de Seguridad de la Información* del CSIC, que decidirá al respecto.

En el marco de sus competencias, el *Responsable de la Información y del Servicio* además ejercerá las siguientes funciones:

a) Definición del uso de la información de la que es responsable dentro y fuera del CSIC.

b) Análisis y gestión de los riesgos asociados al uso de esta información, en coordinación con el *Responsable del Sistema*.

c) Clasificación de la información basándose en su sensibilidad y criticidad, según los criterios de clasificación establecidos en el CSIC.

d) Aprobación o denegación de las solicitudes de acceso a la información de la que es responsable y coordinación de la revisión periódica de los permisos asignados.

En caso de incumplimiento de las funciones asignadas les serán de aplicación las sanciones indicadas en la correspondiente Normativa o en el Reglamento de Régimen disciplinario de los funcionarios de la Administración del Estado.

b) Responsable de la Información diferenciado del Responsable del Servicio.

El *Responsable del Servicio* estará diferenciado del *Responsable de la Información* cuando se trate de un servicio que maneje información procedente de diversas fuentes -no necesariamente de la misma unidad departamental que la que presta el servicio- o bien, si la prestación del servicio no depende de la unidad responsable de la Información.

En estos dos supuestos, el perfil de *Responsable de la Información* no podrá coincidir con el de *Responsable del Servicio* salvo que exista un acuerdo previo que así lo permitiera entre las personas o unidades potencialmente implicadas en ello respecto del servicio y de la información.

c) Responsable del Tratamiento.

En todos aquellos casos en los que como parte del servicio y de la información manejada por el mismo se produzcan tratamientos de datos de carácter personal, dicho tratamiento habrá de cumplir lo establecido en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

En este sentido, el rol de *Responsable del Tratamiento* que establece la ley mencionada en el párrafo anterior se corresponderá, con carácter general, con el de *Responsable de la Información* (o *Responsable de la*

Información y del Servicio) conforme se definen en el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad y de acuerdo a lo establecido en los puntos a) y b) anteriores.

2.3.3 Nivel de operación.

a) Responsable del Sistema.

El *Responsable del Sistema* será la persona encargada de almacenar y proteger la información en los sistemas y redes del CSIC, de acuerdo con la legislación vigente, la normativa y directrices técnicas fijadas por esta Agencia Estatal.

En la Organización Central, la Secretaría General Adjunta de Informática será la encargada de designar al *Responsable del Sistema*. En los institutos y centros, la designación corresponderá al Gerente. En todo caso, la designación se registrará en la documentación de seguridad del sistema de información.

El perfil de *Responsable del Sistema* deberá desempeñarse, en todo caso, por personal del CSIC; sólo muy excepcionalmente podrán asignarse tareas específicas de este perfil a personal ajeno a la Institución perteneciente a la plantilla de alguna empresa contratista.

Con carácter general y siempre que sea posible, las funciones del *Responsable de Seguridad* y del *Responsable del Sistema* no deben ser ejercidas por la misma persona.

El *Responsable del Sistema* asumirá las siguientes responsabilidades en materia de seguridad:

a) Desarrollar, gestionar y mantener el Sistema de Información, entendiendo como tal cualquier aplicación, servicio o recurso informático en sentido amplio, durante todo su ciclo de vida, así como verificar sus especificaciones, instalación y correcto funcionamiento.

b) Definir la arquitectura y sistema de gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo.

c) Verificar que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.

d) Elaborar la configuración de seguridad de la información que aplicarán los *Administradores de la Seguridad de los Sistemas*.

e) Redactar la documentación de seguridad del sistema.

f) Si se detectasen deficiencias graves de seguridad, deberá acordar la suspensión del acceso y gestión de la información, equipo afectado o prestación de un servicio. Esta decisión deberá consensuarse con los responsables de la información en riesgo o bien con el *Comité de Seguridad del Centro o Institut*, y con la *Oficina Técnica de Seguridad,* que en todo caso deberá ser informada de dichas deficiencias de seguridad detectadas.

En aquellos sistemas de información en los que, por su complejidad, distribución, separación física de sus elementos o número de usuarios, se necesite personal adicional para llevar a cabo las funciones de *Responsable del Sistema*, se podrán designar los *Responsables Delegados de Sistemas* que se precisen. La designación corresponderá al *Responsable del Sistema*, quien podrá delegar el desempeño de determinadas funciones, pero nunca la responsabilidad. Los delegados se harán cargo, en su ámbito, de todas aquellas acciones que les hayan sido delegadas y que en general, estarán relacionadas con la operación, mantenimiento, instalación y verificación del correcto funcionamiento del Sistema de información. Cada delegado deberá informar convenientemente al *Responsable del Sistema*, de quien dependerá funcionalmente.

Los *Responsables del Sistema* y *Responsables Delegados de Sistemas* formarán parte de la División a la que corresponda funcionalmente el recurso o sistema a administrar y securizar.

De forma transitoria, hasta la completa implantación del nuevo modelo de gobernanza TIC, el rol de *Responsable del Sistema* por defecto será asumido por la persona que ejerza las funciones de *responsable TIC del ICU.*

En caso de incumplimiento de las funciones que le correspondan serán de aplicación las sanciones indicadas en la correspondiente Normativa o en el Reglamento de Régimen disciplinario de los funcionarios de la Administración del Estado.

b) Administrador de Seguridad del Sistema.

La persona o personas designadas como *Administrador de Seguridad del Sistema* (ASS) dependerán funcionalmente del *Responsable del Sistema*, sin perjuicio del rol coordinador, supervisor y validador de dicha seguridad que tiene la Oficina Técnica de Seguridad de la Información.

En cualquier caso, se podrán segregar las funciones del ASS de un determinado recurso para que se desempeñen por personas diferentes; una encargada del aseguramiento de la prestación del servicio y otra encargada de la protección de la información.

Los distintos *Administradores de la Seguridad del Sistema* formarán parte de la División a la que corresponda funcionalmente el recurso o sistema a administrar y securizar, en consonancia con la adscripción del *Responsable del Sistema* del que dependan.

De forma transitoria, hasta la completa implantación del nuevo modelo de gobernanza TIC, el rol de *Administrador de la Seguridad del Sistema* por defecto será asumido por personal que administre dicho recurso en el ICU, pudiendo recaer, especialmente en casos de ICU con poco personal, en el propio *Responsable del Sistema.*

En el ámbito de la Secretaría General Adjunta de Informática los *Administradores de la Seguridad del Sistema* serán los técnicos adscritos a cada una de las áreas de dicha Secretaría General Adjunta que se encarguen de la administración, gestión y securización de los recursos administrados por dicha área.

El ASS tendrá las siguientes funciones:

a) Implantación, gestión y mantenimiento de las medidas de seguridad aplicables al Sistema de Información.

b) La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad del Sistema de Información.

c) La gestión de las autorizaciones concedidas a los usuarios del sistema, en particular los privilegios concedidos, incluyendo los controles necesarios para que la actividad desarrollada en el sistema se ajuste a lo autorizado.

d) La aplicación de los Procedimientos Operativos de Seguridad.

e) Aprobar los cambios en la configuración vigente del Sistema de Información.

f) Asegurar el estricto cumplimiento de los controles de seguridad establecidos.

g) Asegurar la aplicación de los procedimientos aprobados para manejar el sistema de información.

h) Supervisar las instalaciones de hardware y software, así como sus modificaciones y mejoras para asegurar que la seguridad no está comprometida y se adecúa a las autorizaciones pertinentes.

i) Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos y mecanismos de auditoría técnica implantados en el sistema.

j) Informar al *Responsable del Sistema* del que dependen y a la *Oficina Técnica de Seguridad* de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.

k) Colaborar en la detección, investigación y resolución de incidentes de seguridad.

l) Salvaguardar el almacenamiento y procesamiento seguro de la información, como puede ser el backup de la información y la administración de los sistemas de control de accesos.

Asimismo, si se produjeren incidentes de seguridad, el ASS deberá:

a) Registrar, contabilizar y gestionar los incidentes de seguridad en los sistemas bajo su responsabilidad.

b) Aislar el incidente para evitar la propagación a elementos ajenos a la situación de riesgo.

c) Mantener y recuperar la información almacenada por el sistema y sus servicios asociados.

d) Determinar el origen, motivación y forma del incidente, en la medida que resulte posible, elaborando el correspondiente informe con todos los detalles oportunos y relevantes que se puedan conocer acerca del mismo.

En caso de incumplimiento de las funciones asignadas se le aplicarán las sanciones indicadas en la correspondiente Normativa o en el Reglamento de Régimen disciplinario de los funcionarios de la Administración del Estado.

c) Usuario

El perfil de *Usuario* será el que corresponda a todo aquel que tenga acceso a la información y/o sistemas del CSIC con independencia del tipo de vinculación que tenga con esta Agencia Estatal.

El perfil del *Usuario* definirá las capacidades de lectura, creación y modificación de la información que posee y cada usuario deberá tener los mínimos privilegios imprescindibles (derechos de acceso) para la adecuada ejecución de su trabajo. En caso de que cambie la necesidad de acceso a la información, los privilegios del usuario deberán ser inmediatamente revocados o modificados, según corresponda.

Este proceso se describirá en la Normativa de Seguridad referente al Control de Acceso.

El *Usuario* de la información tendrá las siguientes obligaciones:

a) Solicitar al propietario o *Responsable de la Información* los accesos a la información y sistemas.

b) No utilizar la información del CSIC para cualquier otro fin distinto al autorizado por el propietario o por su inmediato superior.

c) Manejar de forma segura la información a la que tiene acceso, manteniendo en secreto su clave de acceso y adoptando las adecuadas medidas de seguridad para la manipulación de información sensible en cualquier tipo de soporte.

d) Informar al propietario, o a su superior inmediato, de los errores o anomalías en la información a la que tiene acceso.

En caso de incumplimiento de las obligaciones de usuario se le aplicarán las sanciones indicadas en la correspondiente Normativa o en el Reglamento de Régimen disciplinario de los funcionarios de la Administración del Estado.

Dos. El "Anexo A. Organización de Seguridad en la Organización Central del CSIC" queda redactado del siguiente modo:

Anexo A. Organización de Seguridad en la Organización Central del CSIC

1) Participantes

En la Organización Central del CSIC, la Secretaría General será la responsable de la Seguridad y las siguientes de sus unidades organizativas tendrán competencias relacionadas con la Seguridad de la Información:

- Secretaría General Adjunta de Informática.
- Secretaría General Adjunta de Recursos Humanos.
- Asesoría Jurídica.
- Oficialía Mayor.

Todas estas unidades organizativas reportarán al *Comité Corporativo de Seguridad* en materia de Seguridad de la Información.

2) Funciones y Responsabilidades

▶ Secretaría General

En el marco de la política de seguridad de la información del CSIC, la Secretaría General será la responsable de la seguridad de la información en la ORGC, Organización Central del CSIC, debiendo, asimismo:

a) Difundir las actualizaciones periódicas de la Política de Seguridad de la Información en el CSIC y de cuantas Instrucciones la desarrollen.

b) Colaborar con los responsables de la comunicación en la elaboración de la versión oficial de los posibles incidentes de seguridad.

c) Actuar como órgano de enlace e interlocutor con los responsables generales de la materia, como las Fuerzas y Cuerpos de Seguridad del Estado, en especial la Policía Nacional, la Guardia Civil y el Centro Nacional de Inteligencia.

Dentro de la Secretaría General, la Secretaría General Adjunta de Informática y la de Recursos Humanos, así como la Asesoría Jurídica y la Oficialía Mayor, son unidades con funciones específicas en materia de seguridad de la información en la ORGC conforme a la siguiente distribución de responsabilidades:

▪ Secretaría General Adjunta de Informática

La Secretaría General Adjunta de Informática asume las siguientes funciones y responsabilidades en relación con la Seguridad de la Información del CSIC en el ámbito específico de la Organización Central, sin

perjuicio de la consolidación de todo el personal TIC en la SGAI conforme al modelo de gobernanza definido en el Contrato de Gestión y la prestación centralizada a todos los ICU de los servicios definidos en el correspondiente catálogo.

a) Definir e implantar procedimientos, elaborar guías y estándares que implementen lo establecido en el cuerpo normativo de seguridad de la información, en el ámbito de sus competencias.

b) Diseñar e implantar, desde cada una de las divisiones o áreas que forman parte de la SGAI en el ámbito de los recursos administrados por las mismas, los controles de seguridad necesarios para implementar los requisitos de seguridad de la información definidos por su propietario.

c) Trabajar de forma conjunta con la Oficina Técnica de Seguridad cerciorándose de que todos los requisitos de seguridad de la información son conocidos y están bajo control.

d) Realizar, bajo la coordinación de la Oficina Técnica de Seguridad de la Información, verificaciones con las distintas unidades de la SGAI con responsabilidad en sus respectivos ámbitos funcionales y técnicos, para comprobar la vigencia de las medidas de seguridad de la información adoptadas.

e) Implementar los requisitos para conceder los accesos a los sistemas, recursos, aplicaciones y servicios que han sido aprobados por los correspondientes responsables.

f) Configurar, operar y mantener los sistemas de control de acceso a aplicaciones, servidores, redes y elementos de comunicaciones y de seguridad de acuerdo con las políticas del CSIC.

g) Colaborar con los propietarios de la información de la Organización Central para la revisión de los privilegios de acceso concedidos a los usuarios.

h) Conservar todos los registros de cambios realizados en la configuración, para facilitar la investigación de anomalías y la resolución de incidencias y problemas.

i) Asegurar que sólo se utiliza software autorizado en el entorno de producción y eliminar todo software no autorizado.

j) Monitorizar el estado de los sistemas, servidores, infraestructura de nube privada corporativa, equipamiento de red y equipamiento de seguridad para asegurar que todas las actividades se desarrollan correctamente y poder detectar eventos inusuales.

k) Diagnosticar y corregir problemas que surjan en la operación de los sistemas y del equipamiento de comunicaciones y de seguridad.

l) Mantener y revisar logs, pistas de auditoría, informes de errores y demás registros de actividad que sirvan para detectar accesos y/o acciones no autorizadas, así como para la investigación y resolución de problemas.

m) Notificar inmediatamente al equipo de respuesta ante incidentes, cualquier sospecha de intrusión, ciberataque, sabotaje, etc.

n) Gestionar la realización adecuada de copias de respaldo, incluyendo la definición de procedimientos para su ejecución, para su posterior recuperación y para el envío de soportes a ubicaciones seguras, locales o remotas.

o) Gestionar la manipulación segura y conforme a la normativa vigente de los soportes de copias de seguridad, garantizando que sólo el personal autorizado tiene acceso a los mismos.

p) Mantener la seguridad física y lógica de toda la información que resida en los Centros de Procesos de Datos (CPDs) de la Organización Central, permitiendo el acceso sólo al personal autorizado y si fuese necesario, supervisando la actividad del personal externo dentro de los mismos.

q) Investigar cualquier intento de intrusión que se produzca en los CPDs de la Organización Central.

r) Asegurar que la información confidencial que salga del CPD lo hace con las medidas de seguridad y protección requeridas por la Política de Seguridad de la Información en el CSIC y por la normativa vigente.

s) Cualesquiera otras que sean necesarias para asegurar la efectividad de la Política de Seguridad de la Información.

La Secretaría General Adjunta de Informática deberá dar cuenta al *Comité Corporativo de Seguridad* del desarrollo de las funciones indicadas.

- **Secretaría General Adjunta de Recursos Humanos**

La Secretaría General Adjunta de Recursos Humanos será la encargada de:

a) Asegurar la asunción por parte de los trabajadores del CSIC de sus responsabilidades respecto a la seguridad de la información.

b) Ofrecer la información oportuna en el momento de toma de posesión o incorporación a la Organización.

c) Organizar la formación en materia de seguridad de la información

- **Asesoría Jurídica**

La Asesoría Jurídica del CSIC deberá revisar y evaluar periódicamente la normativa que pueda afectar al CSIC en materia de seguridad de la información y recomendar actuaciones a través del *Comité Corporativo de Seguridad de la Información*, así como dar las orientaciones e indicaciones oportunas a ser tenidas en cuenta en materia de protección de los datos de carácter personal que puedan ser tratados.

- **Oficialía Mayor**

Para contribuir a la conformación y aplicación efectiva de la política de seguridad en la información en la ORGC del CSIC, la Oficialía Mayor deberá:

a) Gestionar el sistema de control de acceso a los edificios de la organización central del CSIC, así como el control físico de las llaves de las puertas de los despachos por parte del personal autorizado, disponiendo de copias de las mismas y manteniendo un registro de entrega.

b) Definir recomendaciones para minimizar amenazas relativas a aspectos de seguridad física de los Centros de Proceso de Datos de la Organización Central: fuego, inundación, terremoto, robos, asaltos, etc.

c) Supervisar la instalación, mantenimiento y operación de los sistemas de seguridad física específicos para los CPDs de la ORGC.

d) Realizar revisiones regulares para verificar el cumplimiento de las medidas de seguridad existentes en los CPDs de la ORGC e informar de cualquier anomalía detectada.

e) Supervisar y gestionar el mantenimiento y conservación de las instalaciones de los edificios como climatización, saneamiento, prevención eléctrica, así como los dispositivos de detección (humedad, presencia, alarma y extinción de incendios).

f) Supervisar periódicamente el mantenimiento de las instalaciones y su protección contra el robo, vandalismo, explosión, fuego, inundación, tormentas de viento y otras amenazas, definiendo las recomendaciones encaminadas a minimizar las consecuencias de las eventualidades y llevando un registro de las incidencias.

Sin perjuicio de las funciones y responsabilidades del C*omité Corporativo de Seguridad de la Información*, en la Organización Central se encuentran presentes los distintos roles que el ENS y la presente Organización de la Seguridad establecen.

El *Comité de Seguridad* de la Secretaría General Adjunta de Informática estará compuesto por la persona titular de la SGAI y los responsables de las diferentes divisiones o áreas de la SGAI responsables de los distintos ámbitos técnicos, funcionales y operativos.

La Secretaría General Adjunta de Informática, por la dimensión y variedad de las infraestructuras que gestiona y de los servicios que presta, tanto a la ORGC como a los centros e institutos de investigación, se encuentra estructurada en diversas unidades (divisiones, áreas y servicios) con responsabilidad técnica, funcional y operativa, relativas a los siguientes ámbitos:

1. Seguridad y Comunicaciones
2. Desarrollo
3. Arquitectura Tecnológica
4. Cálculo Científico

5. Microinformática y atención al usuario

La primera de ellas asumirá la responsabilidad del funcionamiento operativo de las redes de comunicaciones y sus servicios asociados, así como de la seguridad perimetral de carácter lógico, siendo el responsable de dicha unidad quien asumirá por defecto el rol de *Responsable de Seguridad* del CSIC, salvo nombramiento específico de otra persona distinta para ocupar dicho rol.

Las cuatro últimas contarán con los correspondientes *Responsables del Sistema*, pudiendo haber en cada uno de dichos ámbitos uno o más *Responsables del Sistema*, o bien nombrar determinados *Responsables del Sistema Delegados*. Entre sus responsabilidades estarán la correcta operatividad de los servicios, infraestructuras y sistemas de carácter corporativo ofrecidos desde la SGAI, entre los que cabe destacar, sin carácter exhaustivo ni exclusivo, los siguientes:

- Desarrollo de aplicaciones
- Intranet corporativa
- Web corporativa y sede electrónica
- Nube privada corporativa
- Infraestructura de escritorio virtual (VDI)
- Correo electrónico
- Servicio de almacenamiento corporativo
- Infraestructura de cálculo científico (HPC)
- Equipos físicos de usuario
- Servicio de videoconferencia corporativa
- Centro de Atención al usuario (CAU)
- Otros servicios y recursos

En el Nivel de especificación se encuentran los responsables de las distintas unidades de la Organización Central, tanto de la propia Secretaría General y sus Secretarías Generales Adjuntas como de las distintas Vicepresidencias y Vicepresidencias Adjuntas, que ostentarán los roles de *Responsables de la Información* y *Responsables del Servicio*, cada uno de ellos en sus respectivos ámbitos de responsabilidad respecto de la materia cuya información y/o servicio sean gestionados y operados técnicamente desde la SGAI por los respectivos *Responsables del Sistema* y *Administradores de la Seguridad del Sistema*.

En el Nivel de supervisión se encuentra la Oficina Técnica de Seguridad de la Información.

El Nivel de operación estará compuesto por los distintos *Responsables del Sistema* previamente señalados, así como los *Administradores de la Seguridad del Sistema*, que se corresponderán con el personal TIC que realiza las funciones propias de la operación y administración de los servidores y demás infraestructuras corporativas implicadas en la prestación de los servicios y recursos ofrecidos desde la SGAI a todo el CSIC, tanto a la Organización Central como a los centros e institutos de investigación.

Transitoriamente, hasta la completa implantación del nuevo modelo de gobernanza TIC, el personal de operación indicado en el párrafo anterior se corresponderá con los responsables y técnicos de cada una de las áreas de la SGAI.

Una vez implantado dicho modelo de gobernanza, las áreas o divisiones de la SGAI aglutinarán a un mayor número de técnicos, vinculados en la actualidad a distintos centros e institutos, y que con el nuevo modelo verán difuminada esa actual adscripción a un determinado ICU para pasar a formar parte de la SGAI y a prestar servicios a un abanico potencial de ICU mayor que el actual. Los detalles relativos a dicha adscripción futura serán concretados conforme vaya llevándose a la práctica la puesta en marcha del nuevo esquema organizativo del personal TIC del CSIC.

Tres. Los apartados 2) y 3) del Anexo B se unifican en un único apartado 2), que queda redactado del siguiente modo:

2) Roles y Funciones de Seguridad en servicios en un centro o instituto:

En el Nivel de especificación estarán incluidos los perfiles de *Responsable de la Información* y *Responsable del Servicio*, mientras que en el Nivel de operación se encontrará el *Responsable del Sistema*. Todos ellos formarán parte del *Comité de Seguridad del Centro o Instituto*. Dichos roles podrán ser asumidos de manera colegiada por el citado Comité, o bien se podrán mantener perfiles diferenciados de carácter individual para cada uno de ellos en aquellos casos en los que, por la dimensión del ICU y volumen de personal del mismo resulte viable, en cuyo caso la documentación de seguridad del sistema deberá contener dicha asignación de perfiles y roles.

Además del *Responsable del Sistema*, en el nivel de operación se encuentran los distintos *Administradores de la Seguridad del Sistema*, roles correspondientes a personal adscrito a las divisiones, áreas o servicios técnicos y funcionales directamente relacionados con los distintos sistemas y recursos a securizar y, en paralelo y desde un punto de vista geográfico, adscritos a la Agrupación que preste servicios TIC al ICU en cuestión.

De manera transitorio, hasta la completa implantación del nuevo modelo de gobernanza TIC, las funciones correspondientes a ambos roles serán realizadas por el personal TIC perteneciente al ICU en cuestión, pudiendo en caso de ICU de pequeño tamaño ser coincidente en una misma persona las funciones de *Responsable del Sistema* y de *Administrador de la Seguridad del Sistema*.

La composición del *Comité de Seguridad del Centro o Instituto*, así como la asignación de roles y perfiles podrán ser adaptados teniendo en cuenta las especificidades asociadas a las modificaciones y reformas organizativas que se puedan producir tanto en la estructura gerencial como en la correspondiente a la prestación de servicios TIC vinculada esta última con la implantación del nuevo modelo de gobernanza TIC.

En el Nivel de supervisión se encuentra la Oficina Técnica de Seguridad de la Información.

Las funciones y responsabilidades de los distintos roles, tanto los asumidos de forma colegiada por un comité como los correspondientes a una determinada persona con carácter individual, serán las definidas en el apartado *2.2 - Los agentes responsables en la seguridad de la información: perfiles profesionales*.

DISPOSICIÓN FINAL PRIMERA.- 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,

Ignacio Gutiérrez Llano