RESOLUCIÓN de fecha 31 de enero de 2019, de la Directora- Gerente del Instituto Aragonés de Ciencias de la Salud, por la que se aprueba la Política de Seguridad de la Información del Instituto Aragonés de Ciencias de la Salud, y se crea la Comisión de Seguridad de la Información del Instituto Aragonés de Ciencias de la Salud y la figura del Responsable de Seguridad TIC.

El Instituto Aragonés de Ciencias de la Salud IACS es la entidad que promueve en Aragón el conocimiento en Biomedicina y Ciencias de la Salud. Su creación se sustenta en la Ley 6/2002, de 15 de abril, de Salud de Aragón, que establece en su título IX, que el IACS es una entidad de Derecho Público adscrita al departamento responsable de Salud del Gobierno de Aragón y le dota de personalidad jurídica y patrimonio propio, y plena capacidad para el cumplimiento de los fines de colaboración en el desarrollo de los servicios del Sistema de Salud de Aragón, mediante la formación de los recursos humanos, el fomento de la investigación, la asesoría y cooperación y el aumento del conocimiento sobre la salud de la población y sus determinantes.

La misión del Instituto Aragonés de Ciencias de la Salud es facilitar la promoción de la investigación, la innovación efectiva y la toma de decisiones en los servicios de salud mediante la gestión del conocimiento.

El Instituto Aragonés de Ciencias de la Salud, dentro del ámbito de la seguridad, pretende por la presente, definir la política de seguridad de la información del Instituto Aragonés de Ciencias de la Salud, cuyo objetivo es proporcionar orientación y apoyo a la gestión de la seguridad de la información y los soportes y sistemas que la gestionan de acuerdo a facilitar la innovación efectiva y la toma de decisiones en los servicios de Salud mediante la gestión del conocimiento y dentro del marco de la legislación vigente.

Y todo ello integrando tanto lo regulado por el 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, como por el REGLAMENTO (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

Es por ello que,

SE RESUELVE

Primero.- Aprobar la Política de Seguridad de la información del Instituto Aragonés de Ciencias de la Salud, definida en el documento adjunto a la presente resolución.

Segundo.- En cumplimiento del apartado 8.3 de dicha Política, por la presente se crea la Comisión de Seguridad de la Información del Instituto Aragonés de Ciencias de la Salud, como órgano colegiado, adscrito a la Dirección-Gerencia del IACS, de carácter transversal para la coordinación y gobierno en materia de seguridad de los activos de tecnologías de la información y comunicaciones del IACS. Su misión será alinear las actividades de la organización en materia de seguridad de la información y tecnologías.

Tercero.- Asimismo se crea la figura del Responsable de Seguridad TIC, que formará parte del citado Comité, con las responsabilidades y funciones previstas en dicha Política.

Lo cual se firma a los efectos oportunos, en

Zaragoza, a fecha de (ver fecha de firma electrónica)

Firmado electrónicamente por la
Directora-Gerente del Instituto Aragonés de Ciencias de la Salud,
SANDRA GARCÍA ARMESTO

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

DEL INSTITUTO ARAGONÉS DE CIENCIAS DE LA SALUD

Versión	REALIZADO		APROBADO
1	Grupo de trabajo ad hoc		Dirección Gerencia IACS
	Fecha: 21/11/2018		Ver fecha de firma electrónica

Contenido

1. INTRODUCCIÓN.

El presente documento describe, dentro del ámbito de la seguridad, la política de seguridad de la información del Instituto Aragonés de Ciencias de la Salud, en adelante IACS, cuyo objetivo **es proporcionar orientación y apoyo a la gestión de la seguridad de la información y los soportes y sistemas que la gestionan de acuerdo a facilitar la innovación efectiva y la toma de decisiones en los servicios de Salud mediante la gestión del conocimiento y dentro del marco de la legislación vigente** (véase 3. MARCO LEGAL.).

2. MISIÓN DEL INSTITUTO ARAGONÉS DE CIENCIAS DE LA SALUD.

El Instituto Aragonés de Ciencias de la Salud IACS es la entidad que promueve en Aragón el conocimiento en Biomedicina y Ciencias de la Salud. Su creación se sustenta en la Ley 6/2002, de 15 de abril, de Salud de Aragón, que establece en su título IX, que el IACS es una entidad de Derecho Público adscrita al departamento responsable de Salud del Gobierno de Aragón y le dota de personalidad jurídica y patrimonio propio, y plena capacidad para el cumplimiento de los fines de colaboración en el desarrollo de los servicios del Sistema de Salud de Aragón, mediante la formación de los recursos humanos, el fomento de la investigación, la asesoría y cooperación y el aumento del conocimiento sobre la salud de la población y sus determinantes.

La misión del Instituto Aragonés de Ciencias de la Salud es facilitar la promoción de la investigación, la innovación efectiva y la toma de decisiones en los servicios de salud mediante la gestión del conocimiento.

En el artículo 65, de la citada Ley, se determina que corresponden al Instituto Aragonés de Ciencias de la Salud las siguientes funciones generales:

- Transferencia de conocimiento para la toma de decisiones.
- Desarrollo de guías de práctica de carácter estratégico.
- Desarrollo de los planes de formación continuada de los profesionales sanitarios de carácter estratégico.
- Formación específica en salud pública y disciplinas afines, gestión y administración sanitaria, economía de la salud y metodología de la investigación.
- Formación de personal investigador.
- Creación y mantenimiento de un fondo de documentación en ciencias de la salud.
- Diseño de las líneas de investigación relacionadas con las prioridades de salud.
- Promoción y desarrollo de proyectos de investigación en ciencias de la salud.
- Dar soporte a grupos de investigación.
- Diseño y coordinación de estudios de evaluación de los servicios de salud y tecnologías sanitarias.
- Prestación de servicios y realización de informes y actuaciones que, en el ámbito de su competencia, le sean encomendados por el Departamento responsable de Salud.
- Cualquier otra relacionada con el fomento de la investigación, la asesoría, la cooperación y el aumento de conocimiento sobre la salud.

La normativa prevista en el siguiente apartado, así como los convenios de colaboración que el IACS ha venido firmando desde su creación con distintas instituciones públicas y privadas, desarrollan y concretan asimismo diversas funciones específicas del IACS.

3. MARCO LEGAL.

El marco legal aplicable al Instituto Aragonés de Ciencias de la Salud, está constituido por el conjunto de leyes y normas de ámbito europeo, nacional y autonómico, que regulan el desarrollo de su actividad y la protección de la información que maneja.

Las normas más destacadas son:

- LEY 14/2007, de 3 de julio, de Investigación biomédica.
- LEY 2/2011, de 4 de marzo, de Economía Sostenible. Sección 1. Transferencia de resultados en la actividad investigadora.
- LEY 14/2011, de 1 de junio, de la Ciencia, la Tecnología y la Innovación.
- LEY 6/2002, de 15 de abril, de Salud de Aragón, por la que se crea el Instituto Aragonés de Ciencias de la Salud como entidad de Derecho Público adscrita al Departamento responsable de Salud.
- CONVENIO-Marco de colaboración entre el Servicio Aragonés de Salud y el Instituto Aragonés de Ciencias de la Salud en materia de investigación, formación de personal y transferencia del conocimiento en biomedicina y ciencias de la salud.
- LEY 9/2003, de 12 de marzo, de fomento y coordinación de la investigación, el desarrollo y la transferencia de conocimientos en Aragón.
- DECRETO 26/2003, de 14 de febrero, del Gobierno de Aragón, por el que se crea el Comité Ético de Investigación Clínica de Aragón.
- REGLAMENTO (UE) nº 536/2014 del Parlamento Europeo y del Consejo, de 16 de abril de 2014, sobre los ensayos clínicos de medicamentos de uso humano, y por el que se deroga la Directiva 2001/20/CE
- REAL Decreto 1090/2015, de 4 de diciembre, por el que se regulan los ensayos clínicos con medicamentos, los Comités de Ética de la Investigación con medicamentos y el Registro Español de Estudios Clínicos
- ORDEN de 12 de abril de 2010, de la Consejera de Salud y Consumo, por la que se regulan los estudios posautorización de tipo observacional con medicamentos en la Comunidad Autónoma de Aragón.
- REAL Decreto 1716/2011, de 18 de noviembre, por el que se establecen los requisitos básicos de autorización y funcionamiento de los biobancos con fines de investigación biomédica y del tratamiento de las muestras biológicas de origen humano, y se regula el funcionamiento y organización del Registro Nacional de Biobancos para investigación biomédica.
- ORDEN de 1 de abril de 2013, del Departamento de Sanidad, Bienestar Social y Familia, por la que se crea el repositorio de datos sanitarios para la Investigación en el Instituto Aragonés de Ciencias de la Salud. (vigencia condicionada por ORDEN SAN/1355/2018).
- ORDEN SAN/1355/2018, de 1 de agosto, por la que se crea la plataforma de información BIGAN como elemento del Sistema de Información de Salud de Aragón.

- REGLAMENTO (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- LEY 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- 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.

4. ÁMBITO DE APLICACIÓN.

La política de seguridad del Instituto Aragonés de Ciencias de la Salud, en adelante IACS, será de aplicación a toda la información que se genere, utilice, procese, transforme o almacene, dentro de la organización del IACS, en el desarrollo de su actividad.

La información es uno de los activos más importantes de la actividad del IACS y se extiende su concepto tanto a la información tangible (incluye el formato digital como ficheros almacenados en medios electrónicos y ópticos, y el formato material como el papel) como la información intangible (incluyendo el conocimiento de los empleados).

5. ALCANCE.

La política de seguridad se aplica a las distintas dimensiones de la información: confidencialidad, disponibilidad, integridad, calidad y trazabilidad. Implica la aplicación de una serie de controles y de gestión de riesgos. Debe adaptarse a las características de la información y a los objetivos del IACS.

Se da en la presente versión relevancia a la información tangible en formato electrónico quedando la definición de la política de seguridad de otras modalidades de la información pendiente de desarrollo en versiones posteriores.

La política de seguridad abarcará también a los soportes y sistemas que almacenen o administren la información.

6. A QUIÉN VA DIRIGIDA.

Este documento está dirigido a toda persona, independientemente de su relación laboral, que tenga acceso, directa o indirectamente, a información del IACS, incluidos los sistemas de comunicaciones que sustentan la transferencia de información, así como los aplicativos utilizados para su proceso y almacenamiento.

7. DESCRIPCIÓN DE LA POLÍTICA DE SEGURIDAD TIC.

7.1. Objetivos de la política de seguridad de las tecnologías de la información y las comunicaciones.

La política de seguridad de las tecnologías de la información y comunicaciones del Instituto Aragonés de Ciencias de la Salud, en adelante, política de seguridad TIC del IACS, persigue la consecución de los siguientes objetivos:

a) Garantizar a todos los usuarios del IACS y clientes que sus datos serán gestionados de acuerdo a los estándares y buenas prácticas en seguridad TIC.
b) Aumentar el nivel de concienciación en materia de seguridad TIC de todos los destinatarios a las que es de aplicación la Política, promoviendo que el personal a su servicio es consciente de sus obligaciones y responsabilidades.
c) Establecer las bases de un modelo integral de gestión de la seguridad TIC en el IACS, que cubra un ciclo continuo de mejora los aspectos técnicos, organizativos y procedimentales.
d) Cumplir con la legislación vigente en materia de seguridad TIC y en concreto al Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad. También se tendrá en consideración el Reglamento (UE) 2016/679 de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales.
e) Hacer patente el compromiso del IACS con la seguridad de la información mediante su apoyo a la **Comité de Seguridad de la Información del IACS** (ver apartado 8.3. Comité de Seguridad de la información del IACS.) dotándole de los medios y facultades necesarias para la realización de sus funciones.
f) Definir, desarrollar y poner en funcionamiento los controles metodológicos técnicos, organizativos y de gestión, necesarios para garantizar de un modo efectivo y medible la preservación de los niveles de confidencialidad, disponibilidad e integridad de la información aprobados por el IACS.
g) Garantizar la continuidad de los servicios ofrecidos por el IACS a sus usuarios y clientes.
h) Crear y promover de manera continua una "cultura de seguridad" tanto internamente, a todo el personal, como externamente a los clientes y proveedores que permita asegurar la eficiencia y eficacia de los controle implantados y aumente la confianza de nuestros clientes.

7.2. Principios de la política de seguridad TIC.

La política de seguridad TIC del IACS se desarrollará, con carácter general, de acuerdo a los siguientes principios:

a) **Principio de confidencialidad**: los activos TIC deberán ser accesibles únicamente para aquellas personas usuarias, órganos y entidades o procesos expresamente autorizados para ello, con respecto a las obligaciones de secreto y sigilo profesional.
b) **Principio de integridad y calidad**: se deberá garantizar el mantenimiento de la integridad y calidad de la información, así como de los procesos de tratamiento de la misma, estableciéndose los mecanismos para asegurar que los procesos de creación,

tratamiento, almacenamiento y distribución de la información contribuyen a preservar su exactitud y corrección.

c) **Principio de disponibilidad y continuidad**: se garantizará un alto nivel de disponibilidad en los activos TIC y se dotarán de los planes y medidas necesarias para asegurar la continuidad de los servicios y la recuperación ante posibles contingencias graves.

d) **Principio de trazabilidad**: se implantarán medidas para asegurar que en todo momento se pueda determinar quién hizo qué y en qué momento con el fin de tener capacidad de análisis sobre los incidentes de seguridad detectados.

e) **Principio de autenticidad**: se deberá articular medidas para garantizar la fuente de información de la que proceden los datos y que las entidades donde se origina la información son quienes dicen ser.

f) **Principio de gestión del riesgo**: se deberá articular un proceso continuo de análisis y tratamiento de riesgos como mecanismo básico sobre el que debe descansar la gestión de la seguridad de los activos TIC.

g) **Principio de proporcionalidad en coste**: la implantación de medidas que mitiguen los riesgos de seguridad de los activos TIC deberá hacerse bajo un enfoque de proporcionalidad en los costes económicos y operativos.

h) **Principio de concienciación y formación**: se articularán iniciativas que permitan a las personas usuarias conocer sus deberes y obligaciones en cuanto al tratamiento seguro de la información se refiere. De igual forma, se fomentará la formación específica en materia de seguridad TIC de todas aquellas personas que gestionan y administran sistemas de información y telecomunicaciones.

i) **Principio de prevención**: se desarrollarán planes y líneas de trabajo específicas orientadas a prevenir fraudes, incumplimientos o incidentes relacionados con la seguridad TIC.

j) **Principio de mejora continua**: se revisará el grado de eficacia de los controles de seguridad TIC implantados, al objeto de adecuarlos a la constante evolución de los riesgos y del entorno tecnológico de la Administración del Gobierno de Aragón.

k) **Principio de seguridad TIC en el ciclo de vida de los activos TIC**: las especificaciones de seguridad se incluirán en todas las fases del ciclo de vida de los servicios y sistemas, acompañadas de los correspondientes procedimientos de control.

l) **Principio de función diferenciada**: en los sistemas de información se diferenciará el responsable de la información, el responsable del servicio y el responsable de la seguridad. El responsable de la información determinará los requisitos de los servicios prestados; y el responsable de seguridad determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios. Las atribuciones de cada responsable y los mecanismos de coordinación y resolución de conflictos serán objeto de desarrollo con el fin de quedar debidamente acotados y reflejados documentalmente.

8. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN DEL IACS.

8.1. Responsabilidad general.

La preservación de la seguridad de la información será considerada objetivo común de todas las personas a los que se dirige este documento (véase 6. A QUIÉN VA DIRIGIDA.), siendo estas responsables del uso correcto de los activos de tecnologías de la información y comunicaciones puestos a su disposición.

8.2 Responsabilidad específica.

La gestión de los procesos de seguridad recogidos en el Sistema de Gestión de la Seguridad de Tecnologías de la Información y Comunicaciones (SGSTIC) del IACS es responsabilidad de un conjunto de personas con funciones concretas, definidas y documentadas. El personal que desempeñe tareas específicas relacionadas con la seguridad de la información y de las tecnologías de la información y comunicaciones recibirá la formación adecuada que se ajuste a sus funciones y nivel de responsabilidad. Para una mejor respuesta ante incidentes de seguridad, el IACS mantendrá relaciones de cooperación en materia de seguridad con las autoridades competentes, el Departamento de Sanidad de quién orgánicamente depende, otros Departamentos y entidades del Gobierno de Aragón, proveedores de servicios informáticos o de comunicación, así como organismos públicos o privados dedicados a promover la seguridad de los sistemas de información.

8.3. Comité de Seguridad de la información del IACS.

Se creará el Comité de Seguridad de la Información del IACS, así como la creación de la figura del Responsable de Seguridad TIC (ver apartado 8.4. Responsable de Seguridad TIC.), que formará parte del citado Comité.

El Comité de Seguridad de la Información del IACS se creará como órgano colegiado, adscrito a la Dirección-Gerencia del IACS, de carácter transversal para la coordinación y gobierno en materia de seguridad de los activos de tecnologías de la información y comunicaciones del IACS. Su **misión** será alinear las actividades de la organización en materia de seguridad de la información y tecnologías.

El Comité de Seguridad de la Información del IACS se compondrá de un mínimo de 7 y hasta un máximo de 11 miembros, entre los cuales estarán incluidos, presidente, secretario y vocales. Estará **formado** por al menos un miembro de la Dirección del IACS, el Responsable de Seguridad TIC, que actuará como Secretario del Comité de Seguridad de la Información, al menos un investigador y trabajadores de las unidades del IACS: Sistemas de Información, Infraestructuras y equipamiento, Jurídica-Legal y Recursos Humanos. La designación y cese de los miembros del Comité se efectuará mediante resolución de la Dirección-Gerencia del IACS.

El Comité de Seguridad de la Información, en lo regulado en la presente Política de Seguridad, se regirá por lo dispuesto para los órganos colegiados en la Sección 3ª del Capítulo II de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

Serán funciones propias del Comité:

- Velar por la actualización y vigencia de la Política de Seguridad de la Información.
- Definir, aprobar y realizar el seguimiento de planes estratégicos, objetivos e iniciativas en materia de seguridad de la información.
- Velar por la disponibilidad de los recursos necesarios para desarrollar los planes estratégicos y las iniciativas definidos.
- Elevar propuestas de revisión del marco normativo de seguridad TIC al órgano competente para su reglamentaria tramitación.
- Elaboración de informes y propuestas de cumplimiento legal y normativo.
- Establecer directrices comunes y supervisar el cumplimiento de la normativa en materia de protección de datos, seguridad de la información y de seguridad TIC.
- Supervisar y aprobar el nivel de riesgo y de la toma de decisiones en la respuesta de incidentes de seguridad TIC que afecten a los activos del IACS.
- Elaboración y propuesta del planteamiento técnico y operativo de los objetivos e iniciativas en seguridad de la información.
- Coordinación en materias de seguridad de la información.
- Desarrollo y seguimiento de programas de formación y concienciación en materia de seguridad de la información.
- Asesoramiento y soporte en materia de Protección de Datos y seguridad de la información.

El Comité se reunirá al menos una vez por semestre y se regirá por esta Política de Seguridad de la Información.

Como respuesta a incidentes de la información, el Comité tendrá entre sus funciones la toma urgente de decisiones en caso de contingencia grave que afecte a la seguridad de sistemas de información críticos del IACS.

El Comité podrá invitar a participar en sus reuniones a todos aquellos profesionales que considere oportuno, quiénes asistirán con voz y sin voto a las reuniones que se celebren, y estarán obligados a respetar la confidencialidad de la información que reciban en todo momento.

8.4. Responsable de Seguridad TIC.

Para la gestión de la seguridad de la información del IACS, la Dirección-Gerencia nombrará a un Responsable de Seguridad TIC entre profesionales de la misma.

Las responsabilidades y funciones del Responsable de Seguridad TIC se circunscriben a los aspectos relacionados con las TIC y, en concreto, son:

- Mantener el nivel adecuado de seguridad de la información manejada por el IACS y de los servicios prestados por los sistemas TIC.
- Realizar o promover las auditorías periódicas que permitan verificar y adecuar la eficacia del sistema de seguridad del IACS a la constante evolución de los riesgos y sistemas de protección, proponiendo un replanteamiento de la seguridad si fuera necesario.
- Supervisar la adecuación del plan de formación y concienciación a las necesidades de seguridad de las TIC.

- Verificar que las medidas de seguridad establecidas son adecuadas para la protección de la información manejada en el IACS y los servicios prestados.
- Analizar, completar y aprobar toda la documentación relacionada con la seguridad del sistema del IACS.
- Monitorizar el estado de seguridad del sistema del IACS, proporcionando las herramientas de gestión de eventos de seguridad y mecanismos de auditoría implementados en el sistema.
- Apoyar y supervisar la investigación de los incidentes de seguridad desde su notificación hasta su resolución.
- Elaborar informes periódicos de seguridad para el Comité de Seguridad de la Información y la Dirección-Gerencia del IACS donde se incluyan los incidentes más relevantes del periodo, así como el estado del sistema y actuaciones relacionadas con la seguridad TIC de los activos del IACS.
- Proponer la inclusión, adecuación y clasificación de Sistemas de Información que forman parte de los activos del IACS, así como evaluar y gestionar los riesgos que atañen a los mismos para determinar el impacto de las amenazas. No obstante, el establecer las valoraciones respecto a la categoría de cada sistema de información, será función de los responsables de cada sistema de información o servicio, según designa el artículo 44 del RD 3/2010.

[Relación con el Comité de Seguridad de la Información del IACS]

- Ser Secretario del Comité de Seguridad de la Información del IACS.
- Asistir a las reuniones del Comité de Seguridad de la Información del IACS.
- Levantar acta de las conclusiones acordadas en las reuniones con el Comité de Seguridad de la Información del IACS.
- Asesorar y dar soporte al Comité de Seguridad de la Información en materia de seguridad TIC elevando propuestas e informes y elaborando los procedimientos que sean necesarios.

[Relación con el Departamento de Sanidad, Delegado de Protección de Datos]

- Coordinarse con el Departamento de Sanidad y los servicios corporativos del Gobierno de Aragón en materia de seguridad de los sistemas de información del IACS y, en particular, en la seguridad de la información manejada.
- Canalizar la relación con el Delegado de Protección de Datos designado por el IACS, así como solicitar la asistencia del Delegado de Protección de Datos cuando sea necesario. Canalizar la relación con el Servicio competente en materia de seguridad de la información del Departamento de Sanidad en materia de protección de datos de la Comunidad Autónoma de Aragón.

8.5. La seguridad como objetivo corporativo del IACS.

Todo el personal del IACS deberá prestar su colaboración en el desarrollo, la implementación y la mejora continua de la Política de Seguridad de la Información.

9. NORMATIVA Y GESTIÓN DE LA DOCUMENTACIÓN.

La gestión de la seguridad de la información en el Instituto Aragonés de Ciencias de la Salud viene determinada por la legislación vigente en materia de Seguridad de la Información y

Tratamiento de Datos Personales, así como por la normativa específica del propio instituto, constituida por la presente política, y por las normas, estándares y procedimientos operativos que la desarrollan.

El Comité de Seguridad de la Información se encargará de la gestión de los documentos de la normativa, asegurando que ésta sea completa y proporcione información suficiente para definir las necesidades de protección de la información y procedimentar su gestión con las debidas garantías, en el ámbito del Instituto Aragonés de Ciencias de la Salud.

Los documentos de la normativa de seguridad del IACS serán publicados y divulgados con el objetivo de que sean conocidos y aplicados por todos los usuarios afectados. La política de seguridad y aquellos documentos que sean de relevancia para el público general, se harán accesibles a través del portal institucional del IACS.

La normativa de seguridad del IACS estará formada, al menos, por los siguientes documentos:

1.- La presente Política de Seguridad

2.- Normativas generales:

2.a. - Política de acceso físico

2.b.- Política de acceso lógico (sistemas y servicios)

2.c.- Política de acceso para proveedores externos

2.d.- Medidas de seguridad TIC

2.e.- Políticas de uso de Puesto de Trabajo Informático

2.f.- Procedimientos de seguridad

3.- Normativas específicas:

Normativas y protocolos específicos de los distintos servicios del IACS, entre los que se pueden destacar:

- BIGAN
- Actividad de investigación/innovación
- CEICA
- SCTs
- Biobanco
- Recursos humanos
- Cualquier otra aplicable que se considere oportuna.

4.- Registros y documentos periódicos:

Entendidos como la documentación operativa que es necesaria para garantizar la seguridad de la información.

4.a. - Inventario y valoración de activos

4.b.- Registro de actividades de tratamiento de datos

4.c.- Análisis de riesgos

4.d.- Auditorías de seguridad

4.e.- Registro de incidencias de seguridad

10. GESTIÓN DE RIESGOS.

Todos los sistemas afectados por esta Política de Seguridad de la Información están sujetos a un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá periódicamente o cuando se de alguna de estas circunstancias: cambie la información manejada, cambien los servicios prestados, suceda un incidente grave de seguridad o se detecten vulnerabilidades graves.

Para armonizar los análisis de riesgos, el Comité de Seguridad de la Información establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados.

11. REVISIÓN DE LA POLÍTICA DE SEGURIDAD.

La presente Política de Seguridad de la información estará sujeta a una revisión y adecuación dentro de una filosofía de desarrollo y mejora continua.