POLÍTICA DE SEGURIDAD DE LA INFORMACIÓNDEL INSTITUTO ARAGONÉS DE CIENCIAS DE LA SALUD

Versión	REALIZADO	APROBADO	APROBADO
3	Grupo de trabajo ad hoc	Comité de Seguridad de la información del IACS.	Dirección Gerencia IACS
	Fecha: 15/05/2024	Fecha: 21/05/2024	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, entre otras, 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 17/2018, de 4 de diciembre, de Investigación e Innovación de 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.

- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- Ley 5/2021, de 29 de junio, de Organización y Régimen Jurídico del Sector Público Autonómico de Aragón.
- Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014.
- DECRETO-LEY 2/2023, de 22 de noviembre, del Gobierno de Aragón, por el que se modifica la Ley 11/2023, de 30 de marzo, de uso estratégico de la contratación pública de la Comunidad Autónoma de Aragón.
- Real Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto Básico del Empleado Público.
- Convenio Colectivo del Instituto Aragonés de Ciencias de la Salud.
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

4. ÁMBITO DE APLICACIÓN.

La política de seguridad del 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 u organización, independientemente de su relación laboral o de otro tipo con el IACS, 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. DATOS DE CARÁCTER PERSONAL

Será de aplicación lo dispuesto en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales; y lo dispuesto en la normativa europea, nacional y autonómica aplicable a tales efectos.

Cada departamento se encargará de gestionar y mantener la seguridad referente a los datos de carácter personal incluidos en las operaciones de tratamiento que a tal efecto sean de su responsabilidad.

Todos los sistemas de información de IACS se ajustarán a los niveles de seguridad requeridos por esta normativa.

8. DESCRIPCIÓN DE LA POLÍTICA DE SEGURIDAD TIC.

8.1. 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 IACS, 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 los que es de aplicación la Política, promoviendo que el personal a su servicio sea 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 el Real Decreto 311/2022, de 3 de mayo, 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, y lo dispuesto en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
e) Hacer patente el compromiso del IACS con la seguridad de la información mediante su apoyo al Comité de Seguridad de la Información del IACS (ver apartado 11.3. 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.

8.2. Principios de la política de seguridad TIC (principios básicos del ENS).

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

a) **Seguridad como proceso integral**: la seguridad se entiende como un proceso integral constituido por todos los elementos humanos, materiales, técnicos, jurídicos y organizativos relacionados con el sistema de información. Se prestará atención a la concienciación de las personas para evitar que la ignorancia, la falta de organización y de coordinación, constituyan fuentes de riesgo.
b) **Gestión de la seguridad basada en los riesgos**: 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.
c) **Prevención, detección, respuesta y conservación**: se desarrollarán planes y líneas de trabajo específicas orientadas a prevenir fraudes, incumplimientos o incidentes relacionados con la seguridad. De igual manera, el sistema mantendrá disponibles los servicios durante todo el ciclo vital de la información digital.
d) **Vigilancia continua y reevaluación periódica**: la vigilancia continua detectará actividades anómalas a las que dará respuesta. Los controles de seguridad implantados, se reevaluarán al objeto de adecuar su eficacia a la constante evolución de los riesgos, de los sistemas de protección y del entorno tecnológico.
e) **Diferenciación de responsabilidades**: la responsabilidad de la seguridad de los sistemas estará diferenciada de la responsabilidad de seguridad, así como de la responsabilidad de la información y la responsabilidad del servicio. Los roles y responsabilidades de cada una de estas funciones deberán quedar debidamente acotadas y reflejadas documentalmente.

8.3. Requisitos Mínimos de Seguridad

Esta Política de Seguridad se establecerá de acuerdo con los principios básicos indicados y se desarrollará aplicando los siguientes requisitos mínimos:

a) Organización e implantación de un Sistema de Gestión de seguridad: la seguridad de los sistemas de información compromete a todos los miembros de IACS. Así mismo, la estructura organizativa establecida en IACS, cumplirá el principio de Diferenciación de Responsabilidades.
b) Análisis y gestión de los riesgos: el análisis y gestión de riesgos será parte esencial del proceso de seguridad. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, el impacto y la probabilidad de los riesgos a los que estén expuestos y la eficacia y el coste de las medidas de seguridad.
c) Gestión del personal: se implantarán los mecanismos necesarios para que cualquier persona que acceda, o pueda acceder a los activos de información, conozca sus responsabilidades y de este modo se reduzca el riesgo derivado de un uso indebido de dichos activos.
d) Profesionalidad: la seguridad de los sistemas estará atendida, revisada y auditada por personal cualificado, dedicado e instruido en todas las fases de su ciclo de vida. El personal recibirá la formación específica necesaria para garantizar la seguridad de las tecnologías de la información aplicables. Se exigirá, de manera objetiva y no discriminatoria, que los prestadores de servicios de seguridad cuenten con

profesionales cualificados y con unos niveles idóneos de gestión y madurez en los servicios prestados.

e) Autorización y control de los accesos: se limitará el acceso a los activos de información por parte de usuarios, procesos, dispositivos y otros sistemas de información mediante la implantación de los mecanismos de identificación, autenticación y autorización acordes a la criticidad de cada activo. Además, quedará registrada la utilización del sistema con objeto de asegurar la trazabilidad del acceso y auditar su uso adecuado, conforme a la actividad de la organización.
f) Protección de las instalaciones: los activos de información serán emplazados en áreas seguras, protegidas por controles de acceso físicos adecuados a su nivel de criticidad. Los sistemas y los activos de información que contienen dichas áreas estarán suficientemente protegidos frente a amenazas físicas o ambientales.
g) Adquisición de productos de seguridad y contratación de servicios de seguridad: en la adquisición de productos de seguridad será exigible la certificación de la funcionalidad de seguridad relacionada con el objeto de dicha adquisición, según la categoría del sistema y el criterio del responsable de seguridad. Para la contratación de servicios de seguridad se estará obligado a lo dispuesto en el principio de profesionalidad.
h) Mínimo privilegio: lo sistemas de información se diseñarán y configurarán otorgando los mínimos privilegios necesarios para su correcto desempeño.
i) Integridad y actualización del sistema: la inclusión de elementos físicos o lógicos requerirán autorización formal previa a su instalación en el sistema. También para cualquier modificación de la configuración de hardware y software.
j) Protección de la información almacenada y en tránsito: se prestará especial atención a la información almacenada o en tránsito a través de entornos inseguros, como los equipos portátiles, dispositivos portátiles, soportes de información y comunicaciones sobre redes abiertas o con cifrado débil. También forman parte de la seguridad los procedimientos que aseguren la recuperación y conservación a largo plazo de los documentos electrónicos producidos por IACS. Así como la información en soporte no electrónico que haya sido causa o consecuencia de ellos.
k) Prevención ante otros sistemas de información interconectados: se protegerá el perímetro del sistema de información. También se analizará los riesgos derivados de la interconexión de sistemas y se controlará el punto de unión.
l) Registro de actividad y detección de código dañino: Se registrarán las actividades de los usuarios, reteniendo la información necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa.
m) Incidentes de seguridad: se implantarán los mecanismos apropiados para la correcta identificación, registro y resolución de los incidentes de seguridad. Esta gestión de los incidentes se empleará para la mejora continua de la seguridad del sistema.
n) Continuidad de la actividad: se implantarán los mecanismos apropiados para asegurar la disponibilidad de los sistemas de información y mantener la continuidad de sus procesos de negocio, de acuerdo a las necesidades de nivel de servicio de sus usuarios.
o) Mejora continua del Sistema de Gestión de seguridad: Las medidas de seguridad se reevaluarán y actualizarán periódicamente para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección. La seguridad de la información será atendida, revisada y auditada por personal cualificado, instruido y dedicado.

8.4. Sanciones previstas por incumplimiento

Del incumplimiento de la Política de Seguridad y normas que la desarrollan, podrán derivarse las consiguientes responsabilidades disciplinarias, que se sustanciarán conforme a lo establecido en el Convenio Colectivo del IACS y demás normativa sancionadora aplicable.

9. CONCIENCIACIÓN Y FORMACIÓN

Con la concienciación y formación se busca alcanzar varios objetivos. Por una parte y fundamental la plena conciencia respecto a que la seguridad de la información afecta a todos los miembros de IACS y a todas las actividades y servicios que lo componen.

Por otra parte, y siguiendo el principio de seguridad integral, la articulación de los medios necesarios para que todas las personas que intervienen en el día a día de IACS y sus responsables jerárquicos tengan la sensibilidad adecuada hacia la responsabilidad que conlleva al gestionar información de los ciudadanos y de la propia Administración.

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

10.1. Responsabilidad general.

La preservación de la seguridad de la información será considerada objetivo común de todas las personas a las 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 por el IACS.

10.2 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, como se indica en los apartados siguientes. 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.

10.3. Comité de Seguridad de la información del IACS.

Se creará el Comité de Seguridad de la Información del IACS, así como la figura del Responsable de Seguridad TIC (ver apartado 10.4. 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. Sus integrantes representan a los diferentes riesgos a los que se enfrenta la entidad y que va a

permitir evaluar, decidir y materializar las iniciativas en materia de ciberseguridad. Su misión será alinear las actividades de la organización en materia de seguridad de la información y tecnologías.

Dentro de la Organización de la Seguridad, el Comité de Seguridad establece los controles y salvaguardas necesarios para garantizar la seguridad de los sistemas de información del IACS en sus relaciones con los grupos de interés (empleados, proveedores y terceros en general), previo estudio de los riesgos que, para la seguridad de las plataformas tecnológicas y activos de información, dichas relaciones pudieran originar.

El Comité de Seguridad de la Información, en lo regulado en la presente Política de Seguridad, se regirá para su funcionamiento por su reglamento interno, aprobado por el propio Comité y ratificado por la Dirección del IACS y por lo dispuesto para los órganos colegiados en la normativa aplicable 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 de Seguridad de la Información del IACS se compondrá de un mínimo de 7miembros y hasta un máximo de 11, 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, los Responsables de Seguridad de los proyectos estratégicos, al menos un investigador y trabajadores de las unidades del IACS, para garantizar que los activos de la entidad son debidamente asegurados y el Marco de Cumplimiento aprobado por el Comité de Seguridad es aplicado correctamente. La designación y cese de los miembros del Comité se realizará conforme a los criterios establecidos en su reglamento interno. Su composición se detalla en el Mapa de Registros.

El Comité de Seguridad se reúne con la periodicidad necesaria para aprobar la gestión de la seguridad realizada y establecer las estrategias que en este ámbito han de desarrollarse en el futuro. En todo caso, se reunirá al menos una vez por semestre. El Comité de Seguridad puede reunirse además por uno de los siguientes motivos:

- A petición de uno de los vocales y con la aprobación de su presidente.
- A petición de 2/3 de los vocales.
- En el supuesto de la ocurrencia de una contingencia que pudiera ser calificada como desastre.
- En el supuesto de ocurrencia de una incidencia grave relacionada con datos de carácter personal, a iniciativa del Responsable de Seguridad
- Otros motivos de relevancia para la organización en materia de seguridad.

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.

10.4. Responsable de Seguridad TIC.

Es necesario, en todo caso, la existencia del rol de Responsable de Seguridad que articule las relaciones entre los diferentes roles y garantice, con el apoyo de éstos, la implantación de los diferentes controles y salvaguardas que para la gestión de la seguridad sean diseñados elaborados aprobados y validados. Otro tipo de relaciones de colaboración con terceros, entidades públicas o privadas, autoridades, grupos de interés, asesores, etc. deben ser tenidas en cuenta para la adquisición y distribución del conocimiento suficiente que permita alcanzar una implantación, mantenimiento y revisión adecuados de la Gestión de la Seguridad de la Información.

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:

- Promover y participar en el desarrollo e implantación de la Política de Seguridad, Marco de Cumplimiento, SGSI y, con carácter general, cualquier normativa, procedimiento, estándar y directriz asociado a la seguridad de la información.
- Gestionar la seguridad de la información en línea con las directrices generales que emanan de la Política de Seguridad.
- Establecer canales de comunicación con los diferentes agentes que intervienen en la seguridad de la información.
- Coordinación de responsables técnicos para la implementación de las políticas y procedimientos de seguridad dentro de la organización.
- Gestiona las normativas de seguridad aprobadas por el Comité de Seguridad, así como de aquellos registros de auditoría, registro de eventos, incidencias, inventario, etc. generados por el SGSI. Analizar, completar y aprobar dichas normativas.

- Verificar que las medidas de seguridad establecidas son adecuadas para la protección de la información manejada en el IACS y los servicios prestados.
- Propone al Comité de Seguridad la implantación de cualquier control o salvaguarda que en materia de seguridad pudiera surgir en función de las incidencias ocurridas o necesidades detectadas.
- 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.
- Gestionar la revisión periódicamente de la efectividad de los controles implantados en las Plataformas TI.
- Apoyar y supervisar la investigación de los incidentes de seguridad desde su notificación hasta su resolución.
- Participar activamente en el funcionamiento y mejora del SGSI coordinándose con los responsables de cada sistema de información o servicio.
- Escalar cualquier conflicto o aspecto no resuelto que afecte a varias áreas o unidades al Comité de Seguridad.
- Promover y supervisar la realización del análisis de riesgo de los diferentes sistemas de información del IACS, aportando su visión en el uso de la metodología de análisis de riesgos.
- Presentar los resultados del análisis de riesgos al Comité de Seguridad.
- 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.
- Elabora los informes requeridos al Comité de Seguridad sobre la gestión realizada en materia de seguridad, estrategias a llevar a cabo, auditorías realizadas, incidencias destacables, etc.
- Verificar la vigencia y actualidad de los planes de contingencia, llegado el caso.
- En caso de necesidad por cumplimiento legal, es el responsable del plan de contingencia y, por tanto, debe asegurarse de su comunicación a los responsables afectados, su mantenimiento, gestionar su actualización y la realización de las oportunas pruebas.
- Supervisar la adecuación del plan de formación y concienciación a las necesidades de seguridad de las TIC dirigido a todo el personal.
- Revisar la efectividad de los planes de formación, concienciación y sensibilización del personal en materia de seguridad de la información.
- Coordinarse con el resto de Responsables de Seguridad de proyectos estratégicos del IACS, si procede.
- Mantener contacto con grupos de interés, asesores y autoridades en materia de seguridad informática para mantener actualizados los conocimientos de la compañía en esta materia y promover posibles iniciativas.
- Actuar como contacto de referencia en la organización en aspectos relacionados con la seguridad de la información.
- Reportar cualquier otro aspecto que por su relevancia o criticidad debiera ser conocido por el Comité de Seguridad .

[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.

10.5. 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.

11. 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, donde se definen los objetivos, las estrategias y la política relativa a la seguridad del IACS
2. Normativa de seguridad, donde se establecen los requisitos que se sustentan en la política y se regulan determinados aspectos de la seguridad.
3. Procedimientos, donde se determinan las acciones o tareas a realizar en el desempeño de un proceso relacionado con la seguridad.
4. Instrucciones técnicas de seguridad, donde se determina las acciones o tareas necesarias para completar una actividad o proceso de un procedimiento concreto sobre una parte concreta del sistema de información.

5. Registros, proporcionan una evidencia objetiva del cumplimiento de los requisitos del SGSI.
6. Normativa de uso, documento destinado a usuarios finales con la intención de establecer una regulación específica sobre la utilización de un sistema, tecnología o recurso.

12. 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 a las que están expuestos.
- La probabilidad de que cada una de dichas amenazas se materialice.
- El impacto que tendría la materialización de cada amenaza, considerando, además de los daños producidos en el propio activo, posibles daños personales, pérdidas financieras, de imagen o reputación, interrupciones en el servicio y pérdidas de rendimiento.

Los riesgos que se encuentren por encima del umbral admisible serán gestionados determinando, poniendo en marcha y evaluando, las medidas que permitan disminuirlos.

Este análisis se repetirá periódicamente o cuando se produzca 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.

13. 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.

ANEXO I. GLOSARIO DE TÉRMINOS

- **Activo de tecnologías de la información y comunicaciones**: cualquier información o sistema de información que tenga valor para la organización. Incluye datos, servicios, aplicaciones, equipos, comunicaciones, instalaciones, procesos y recursos humanos.
- **Amenaza**: Circunstancia desfavorable que puede ocurrir y que cuando sucede tiene consecuencias negativas sobre los activos provocando su indisponibilidad, funcionamiento incorrecto o pérdida de valor.
- **Análisis de Riesgos**: Es un proceso que comprende la identificación de activos de información, sus vulnerabilidades y las amenazas a los que se encuentran expuestos, así como la probabilidad de ocurrencia y el impacto de las mismas, a fin de determinar los controles adecuados para tratar el riesgo.
- **Auditoría de Seguridad**: Es el estudio que comprende el análisis y gestión de sistemas llevado a cabo por profesionales en tecnologías de la información (TI) con el objetivo de identificar, enumerar y describir las diversas vulnerabilidades que pudieran presentarse en una revisión exhaustiva de las estaciones de trabajo, redes de comunicaciones, servidores o aplicaciones.
- **Confidencialidad**: Confidencialidad es la propiedad de la información, por la que se garantiza que está accesible únicamente a personal autorizado. La confidencialidad de la información, junto con la integridad y la disponibilidad suponen las tres dimensiones de la seguridad de la información.
- **Contingencia grave**: incidente grave de seguridad TIC cuya ocurrencia causaría la reducción significativa de la capacidad de la organización para atender eficazmente a sus obligaciones fundamentales, el sufrimiento de un daño significativo a los activos de la organización, el incumplimiento material grave de alguna ley o regulación, o un perjuicio significativo de difícil reparación a personas.
- **Dato de carácter personal**: cualquier información numérica, alfabética, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables, tanto la relativa a su identidad (como nombre y apellidos, domicilio, filiación, una fotografía o video, etc...) como la relativa a su existencia y ocupaciones (estudios, trabajo, enfermedades, etc.)
- Ejemplos de datos de carácter personal son las direcciones postales, las cuentas de correo electrónico, el DNI, las altas y bajas médicas, la información financiera y fiscal o la afiliación política.
- Los datos relativos a una persona jurídica (domicilio, denominación social, CIF, etc.) no tienen la consideración de datos de carácter personal, por lo tanto, no le será de aplicación el Reglamento de Protección de Datos.
- **Disponibilidad**: Se trata de la capacidad de un servicio, un sistema o una información, a ser accesible y utilizable por los usuarios o procesos autorizados cuando éstos lo requieran. Junto con la integridad y la confidencialidad son las tres dimensiones de la seguridad de la información.
- **Esquema Nacional de Seguridad:** Regulación a la que están sujetas las administraciones públicas que tiene por objeto establecer la política de seguridad en la utilización de medios electrónicos y está constituido por principios básicos y requisitos mínimos que permitan una protección adecuada de la información

- **Impacto:** Consecuencia de la materialización de una amenaza sobre un activo aprovechando una vulnerabilidad. El impacto se suele estimar en porcentaje de degradación que afecta al valor del activo, el 100% sería la pérdida total del activo.
- **Incidente de seguridad TIC**: suceso, accidental o intencionado, a consecuencia del cual se ve afectada la integridad, confidencialidad o disponibilidad de la información.
- **Integridad:** La Integridad es la propiedad de la información, por la que se garantiza la exactitud de los datos transportados o almacenados, asegurando que no se ha producido su alteración, pérdida o destrucción, ya sea de forma accidental o intencionada. La información debe permanecer correcta (integridad de datos) y como el emisor la originó (integridad de fuente) sin manipulaciones por terceros. La integridad, la disponibilidad y la confidencialidad constituyen las dimensiones clave en la seguridad de la información.
- **Plan director de seguridad**: estrategia y conjunto de iniciativas planificadas, plasmadas en un documento escrito, cuyo objetivo es alcanzar un determinado nivel de seguridad en la organización.
- **Política de seguridad de la información y comunicaciones**: conjunto de directrices plasmadas en un documento escrito, que rigen la forma en que una organización gestiona y protege sus activos de tecnologías de la información y comunicaciones.
- **Riesgo**: estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización. Posibilidad de que se produzca un impacto determinado en un activo, en un dominio o en toda la organización.
- **Servicio**: Conjunto de actividades que buscan satisfacer las necesidades de un cliente.
- **Sistema de información**: conjunto organizado de recursos destinado a recoger, almacenar, procesar, presentar o transmitir la información.
- **Sistema de información crítico**: sistema de información cuyo adecuado funcionamiento es indispensable para el funcionamiento de la organización y el cumplimiento de sus obligaciones fundamentales.
- **Vulnerabilidad**: Debilidad que presentan los activos y que facilita la materialización de las amenazas.