# Política de Seguridad de la Información

Referencia: POL_PoliticaSeguridadInformación_0A.docx

Autor: Área de Seguridad

Fecha de creación: 26/12/2018

Última actualización: 10/04/2019

Versión: 1A

Clasificación: Uso Interno

# Control del Documento

## Registro de cambios

| Versión | Fecha | Autor | Descripción |
|---|---|---|---|
| 00 | 26/12/2018 | CiberGob | Creación y Desarrollo del primer borrador |
| 0A | | Área de Seguridad | Validación del Documento |
| 1A | 04/04/2019 | Comité de Seguridad | Aprobación de la Política |

## Control de revisiones

| Fecha revisión | Revisado por | Área | Próxima revisión |
|---|---|---|---|
| Comité de Seguridad | | | |
| | | | |

## Lista de distribución

| Nombre | Área |
|---|---|
| Oficina de Seguridad | |
| | |

## Control de firmas

| Firmado electrónicamente por el Presidente y el Secretario del Comité de Seguridad | |
|---|---|
| 25448429X OSCAR LOPEZ (R: G99426132) Firmado digitalmente por 25448429X OSCAR LOPEZ (R: G99426132) Fecha: 2019.04.10 11:25:05 +02'00' | Eduardo Pastor Miedes Firmado digitalmente por Eduardo Pastor Miedes Fecha: 2019.04.10 13:16:10 +03'00' |
| Presidente del Comité de Seguridad | Secretario del Comité de Seguridad |

# Índice

# 1 Aprobación y entrada en vigor

Texto aprobado por el Instituto de Investigación Sanitaria Aragón, en adelante IIS Aragón, el día 4 de abril de 2019. Esta Política de Seguridad de la Información es efectiva desde dicha fecha y hasta que sea reemplazada por una nueva Política. La entrada en vigor de la presente Política de Seguridad de la Información del IIS Aragón supone la derogación de cualquier otra que existiera.

# 2 Objetivos y misión del Instituto de Investigación Sanitaria Aragón

El Instituto de Investigación Sanitaria de Aragón (IIS Aragón) se articula en torno a un proyecto científico conjunto que tiene como misión facilitar la generación y aplicación de conocimientos científicos capaces de mejorar la salud de la población.

Los fines del IIS Aragón son:

- Aproximar la investigación básica y aplicada, clínica y de servicios sanitarios.
- Crear un entorno investigador, asistencial y docente de calidad al que queden expuestos los profesionales sanitarios, los especialistas en formación, los alumnos de postgrado, y grado,
- Constituir el lugar idóneo para la captación de talento y la ubicación de las grandes instalaciones científico-tecnológicas.

# 3 Objetivos de la Política de Seguridad

La política de seguridad de las tecnologías de la información y comunicaciones del IIS Aragón, en adelante Política de Seguridad TIC del IIS Aragón, persigue la consecución de los siguientes objetivos:

a) Garantizar a los usuarios que los datos alojados en el IIS Aragón serán gestionados de acuerdo a los estándares y buenas prácticas en seguridad TIC.

b) Aumentar el nivel de concienciación en materia de seguridad TIC allí donde es de aplicación esta Política, garantizando 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 IIS Aragón, que cubra en un ciclo continuo de mejora los aspectos técnicos, organizativos y procedimentales.

e) Hacer patente el compromiso del IIS Aragón con la seguridad de la información mediante su apoyo al Comité de Seguridad 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 IIS Aragón.

g) Garantizar la continuidad de los servicios ofrecidos por el IIS Aragón a los usuarios.

h) Crear y promover de manera continua una “cultura de seguridad” tanto internamente, a todo el personal, como externamente a los ciudadanos y proveedores que permita asegurar la eficiencia y eficacia de los controles implantados y aumente la confianza de nuestros ciudadanos.

# 4 Revisión de la Política

Esta política será revisada al menos una vez al año y siempre que haya cambios relevantes en la organización, con el fin de asegurar que ésta se adecua a la estrategia y necesidades de la misma.

La Política será propuesta y revisada por el Comité de Seguridad y aprobada y difundida por el IIS Aragón para que la conozcan todas las partes afectadas.

En caso de conflictos o diferentes interpretaciones de esta política se recurrirá al Comité de Seguridad para resolución de estos, previo informe propuesta de la unidad de protección de datos.

# 5 Marco Normativo

A los efectos previstos en esta Política, el marco normativo de referencia es el que estipula la legislación vigente en materia de seguridad TIC.

Debido al carácter personal y reservado de la información manejada y a los servicios puestos a disposición de los usuarios, el IIS Aragón desarrolla sus actividades de acuerdo a la normativa vigente en dichas materias, de entre las que actualmente cabe destacar por su especial relevancia:

a) Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

b) Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público

c) 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.

d) Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica

e) Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.

f) 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).

g) Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

h) Ley 59/2003, de 19 de diciembre, de firma electrónica.

i) Real Decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición del documento nacional de identidad y sus certificados de firma electrónica.

j) 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.

k) Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores.

l) 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.

# 6 Ámbito de aplicación

Esta Política será de aplicación y de obligado cumplimiento para todos los usuarios del IIS Aragón; a sus recursos y a los procesos afectados por el ENS y el RGPD, ya sean internos o externos vinculados a la entidad a través de contratos o acuerdos con terceros.

# 7 Principios de seguridad TIC

## 7.1 Principios básicos de la política de seguridad TIC

La política de seguridad TIC del IIS Aragón 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 respeto 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 y de la seguridad integral: 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, reacción y recuperación: 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 o de la reevaluación periódica: 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.

k) Principio de seguridad en el ciclo de vida de los activos TIC o líneas de defensa: 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: la responsabilidad de la seguridad de los sistemas estará diferenciada de la responsabilidad del servicio, así como de la responsabilidad de la información. Los roles y responsabilidades de cada una de estas funciones deberán quedar debidamente acotadas y reflejadas documentalmente.

## 7.2 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 del proceso de seguridad: La estructura organizativa para la gestión de la seguridad de la información será competente para mantener, actualizar y hacer cumplir, la Política de Seguridad de la Información del IIS Aragón, así como para garantizar la implantación del proceso de seguridad en el IIS Aragón.

b) Análisis y gestión de los riesgos: El análisis y gestión de riesgos será parte esencial del proceso de seguridad. La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. 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. Al evaluar el riesgo en relación con la seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales.

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 que atiende, revisa y audita la seguridad de los sistemas 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 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: En la adquisición de productos de seguridad será exigible la certificación de la funcionalidad de seguridad relacionada con el objeto de dicha adquisición, según el criterio del responsable de seguridad y aplicando el principio de proporcionalidad. Para la contratación de servicios de seguridad se estará a lo dispuesto en el principio de profesionalidad.

h) Seguridad por defecto: La seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos relacionados con el sistema. La seguridad de la información debe considerarse como parte de la operativa habitual, estando presente y aplicándose desde el diseño inicial de los sistemas de información.

i) Integridad y actualización del sistema: El sistema informático del IIS Aragón será diseñado y mantenido por el responsable del servicio bajo criterios técnicos, de eficiencia y de seguridad. Todo elemento físico o lógico requerirá autorización formal previa a su instalación

en el sistema. También requerirá autorización formal previa cualquier alteración de la configuración de hardware y software de los equipos o cualquier desinstalación de programas de la plataforma de uso predefinida. Con carácter general, no se instalará software salvo que se disponga de la correspondiente licencia de uso, bien por haberlo adquirido la organización, o bien por tratarse de software libre con una licencia aplicable. En todo caso, será el administrador del sistema quien instale el software una vez se autorice.

j) Protección de la información almacenada y en tránsito.

k) Prevención ante otros sistemas de información interconectados: Se establecerán los procedimientos necesarios para lograr una adecuada gestión de la seguridad, operación y actualización de las Tecnologías de la Información y Comunicaciones. La información que se transmita a través de redes de comunicaciones deberá ser adecuadamente protegida, teniendo en cuenta su nivel de sensibilidad y de criticidad, mediante mecanismos que garanticen su seguridad.

l) Registro de actividad: 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.

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 proceso 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 Organización de la seguridad TIC

## 8.1 Responsabilidad general

La preservación de la seguridad TIC será considerada objetivo común de todas las personas al servicio del IIS Aragón, siendo estas responsables del uso correcto de los activos de tecnologías de la información y comunicaciones puestos a su disposición.

En caso de incumplimiento de las directrices y normativas de seguridad indicadas en la presente política y las obligaciones derivadas de ellas, el IIS Aragón se reserva el derecho de aplicar el régimen disciplinario establecido en el Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores.

Por su importancia dentro de la implementación de la seguridad, quedan desarrolladas en la presente política algunas de las funciones de los órganos que el IIS Aragón estima necesarios para la correcta gestión de la seguridad.

## 8.2 Comité de Seguridad TIC del IIS Aragón

1. Se crea el Comité de Seguridad TIC del IIS Aragón, como órgano colegiado de carácter transversal para la coordinación y gobierno en materia de seguridad.

2. El Comité estará formado por un presidente, un secretario y una serie de vocales que representan las unidades del IIS Aragón.

3. Serán funciones propias del Comité:

a) Definición, aprobación y seguimiento de los objetivos, iniciativas y planes estratégicos en seguridad TIC.

b) Velar por la disponibilidad de los recursos necesarios para desarrollar las iniciativas y planes estratégicos definidos.

c) Elevación de propuestas de revisión del marco normativo de seguridad TIC al órgano competente para su reglamentaria tramitación.

d) Establecimiento de directrices comunes y supervisión del cumplimiento de la normativa en materia de seguridad TIC.

e) Supervisión y aprobación del nivel de riesgo y de la toma de decisiones en la respuesta a incidentes de seguridad que afecten a los activos TIC.

f) Definición y aprobación del modelo de relación con los Comités de Seguridad TIC de las entidades incluidas en el ámbito de aplicación de la Política.

4. El Comité se reunirá al menos una vez por semestre y se regirá por esta política.

5. El Comité nombrará entre sus miembros un grupo de respuesta a incidentes TIC, llamado “Comité de Crisis”, cuya función será la toma urgente de decisiones en caso de contingencia grave que afecte a la seguridad de sistemas de información críticos del IIS Aragón.

6. Las labores de soporte y asesoramiento al Comité serán realizadas por el Responsable de Seguridad TIC y la Oficina de Seguridad TIC.

## 8.3 Responsable de Seguridad TIC

1. El nombramiento del Responsable de Seguridad será potestad del Comité de Seguridad del IIS Aragón**.**

2. La persona Responsable de Seguridad TIC tendrá las siguientes funciones, dentro de su Departamento:

a) Definición y seguimiento de las actuaciones relacionadas con la seguridad TIC de los activos de información de la Entidad y la gestión del riesgo.

b) Asesoramiento y soporte sobre temas de Seguridad.

c) Coordinación en materias de seguridad TIC.

d) Propuesta y seguimiento de programas de formación y concienciación.

e) Reporte al Comité de Seguridad de un informe periódico sobre el estado de la Seguridad TI y las actividades relacionadas.

g) Asunción de las funciones incluidas en los artículos 10, 27.3, 34.6, Anexo II (apartado 2.3) y Anexo III (apartados 2.1.b y 2.2.b) del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

f) Asunción de las funciones incluidas en el Reglamento (UE) 2016/679 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 (Reglamento general de protección de datos).

## 8.4 Oficina de Seguridad TIC

1. La Oficina de Seguridad TIC estará compuesto por técnicos de las diferentes unidades del IIS Aragón, si bien se puede convocar a aquellas personas que la Oficina estime necesarias para el desarrollo de los trabajos encomendados.

2. En esta Oficina de Seguridad TIC estará también el Responsable de Seguridad del IIS Aragón que tendrá funciones sobre la revisión y elaboración de propuestas para ser presentadas y debatidas en el Comité de Seguridad TIC.

3. La Oficina de Seguridad TIC tendrá las siguientes atribuciones:

a) Definición del planteamiento técnico y operativo de los objetivos, iniciativas y planes estratégicos en seguridad TIC, de acuerdo con las directrices del Comité de Seguridad TIC.

b) Elaboración de propuestas relativas a la revisión del marco normativo de seguridad TIC.

c) Elaboración de informes y propuestas de cumplimiento legal y normativo.

d) Elaboración de informes sobre el nivel de seguridad TIC de los activos.

e) Reporte al Comité Seguridad TIC de informes periódicos sobre el estado de la Seguridad TI del IIS Aragón.

4. La Oficina de Seguridad TIC se regirá por esta Política.

## 8.5 Responsables

El Responsable de la Información determina los requisitos de seguridad respecto a la información tratada en el IIS Aragón.

El Responsable del Servicio determina la infraestructura hardware y software del sistema de información, los criterios de uso, los servicios ofrecidos, los formatos y cualquier otro aspecto del funcionamiento del sistema de información del IIS Aragón.

El Responsable de Seguridad determina cómo satisfacer los requisitos de seguridad, tanto de la información como de los servicios ofrecidos, incluyendo la definición de procedimientos de seguridad y, en su caso, la adopción de medidas de urgencia ante posibles deficiencias o amenazas en el IIS Aragón.

El administrador del sistema desarrolla, opera y mantiene el sistema de información del IIS Aragón.

Las discrepancias en materia de seguridad serán resueltas atendiendo al criterio de mayor jerarquía.

Las atribuciones de cada responsable, así como los mecanismos de coordinación y resolución de conflictos se explicitan en la Normativa de Roles y Responsabilidades de Seguridad y la Normativa de la Organización de la Seguridad.

# 9 Desarrollo de la Política de Seguridad

## 9.1 Instrumentos del desarrollo

La Política de Seguridad de la Información del IIS Aragón se desarrollará por medio de instrucciones de servicio y circulares que afronten aspectos específicos. Dichas instrucciones y circulares podrán adoptar alguna de las siguientes modalidades:

Se usarán los siguientes instrumentos:

Normas de seguridad: Uniformizan el uso de aspectos concretos del sistema. Indican el uso correcto y las responsabilidades de los usuarios. Son de carácter obligatorio.

Procedimientos: Concretan flujos de trabajo para la realización de tareas, indicando lo que hay que hacer, paso a paso, pero sin entrar en detalles (de proveedores, marcas comerciales o comandos técnicos). Son útiles en tareas repetitivas.

Instrucciones técnicas (IT): Desarrollan los Procedimientos llegando al máximo nivel de detalle, (indicando proveedores, marcas comerciales y comandos técnicos empleados para la realización de las tareas).

La normativa de seguridad estará disponible en la intranet a disposición de todos los miembros de la organización que necesiten conocerla.

## 9.2 Aprobación de las normativas

En toda la organización, la aprobación de las normas de seguridad se hará de acuerdo a lo dispuesto en la presente política y las normativas específicas que para ello desarrollará el IIS Aragón.

## 9.3 Sanciones previstas por incumplimiento

Del incumplimiento de la Política de Seguridad de la Información y normas que la desarrollan podrán derivarse las consiguientes responsabilidades disciplinarias, que se sustanciarán conforme a lo establecido en la Ley del Estatuto de los Trabajadores sobre régimen disciplinario de los empleados.

## 10 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 del IIS Aragón 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 del IIS Aragón y sus responsables jerárquicos tengan la sensibilidad adecuada hacia la responsabilidad que conlleva al gestionar información de los ciudadanos y de la propia Administración.

## 11 Análisis y Gestión de Riesgos

Todos los sistemas sujetos a esta Política deberán ser sometidos a un análisis y gestión de riesgos, evaluando los activos, amenazas y vulnerabilidades a los que están expuestos y proponiendo las contramedidas adecuadas para mitigar los riesgos. Aunque se precisa un control continuo de los cambios realizados en los sistemas, este análisis se repetirá:

- Al menos una vez al año (mediante revisión y aprobación formal).
- Cuando ocurra un incidente grave de seguridad.

Para el análisis y gestión de riesgos se usará la metodología MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información), elaborada por el Consejo Superior de Administración Electrónica y enfocada a las Administraciones Públicas.

## 12 Seguridad de la información

Se desarrollará una Clasificación de la Información del IIS Aragón de forma que se identifiquen los distintos tipos de información, en base a su sensibilidad, se establezca cómo etiquetar los soportes que la contengan y se determine qué se puede y no se debe hacer con cada nivel de clasificación.

## 13 Datos de Carácter Personal

Será de aplicación lo contemplado en el RGPD y lo dispuesto en la legislación nacional a tales efectos.

Cada unidad y/o grupo de investigación 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 del IIS Aragón se ajustarán a los niveles de seguridad requeridos por esta normativa.

## 14 Obligaciones del personal

Todos los miembros de la organización y las empresas y personas terceras que realicen servicios de cualquier clase contratados por el IIS Aragón o que de alguna manera se presten bajo el control y/o la dirección del IIS Aragón tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad. IIS Aragón es responsable de comunicar la política y las normas, así como de disponer de los medios necesarios para que todo el personal las conozca de forma efectiva, en especial, las que puedan afectar a sus funciones.

Se establecerá un programa de concienciación continúa dirigido a todos los miembros del IIS Aragón, en particular a los de nueva incorporación.

El personal deberá usar los procedimientos de notificación de incidentes de seguridad habilitados a tal efecto, en caso de detectar un posible incidente.

Las personas con responsabilidad en el uso, operación o administración de sistemas de información recibirán formación para el manejo seguro de los sistemas.

## 15 Terceras partes

Cuando el IIS Aragón preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipe de esta Política de Seguridad de la Información, se establecerán canales para el reporte y coordinación de los respectivos Delegados de Protección de Datos y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando el IIS Aragón utilice servicios de terceros o ceda información a terceros, se les hará partícipe de esta Política de Seguridad y de la Normativa de Seguridad que ataña a dichos servicios o información. Dicha tercera parte deberá aceptar el quedar sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias. Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política.

Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad de la Información que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este

informe por los responsables de la información y los servicios afectados, así como del responsable del tratamiento previsto en el RGPD, antes de seguir adelante.

# 16 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.

Contingencia grave: Incidente 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 de alguna ley o regulación, o un perjuicio significativo de difícil reparación a personas.

Incidente de seguridad TIC: Suceso, accidental o intencionado, a consecuencia del cual se ve afectada la integridad, confidencialidad o disponibilidad 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.

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.