DEPARTAMENTO DE SANIDAD, BIENESTAR SOCIAL Y FAMILIA

ORDEN de 16 de marzo de 2015, del Consejero de Sanidad, Bienestar Social y Familia, por la que se aprueba la Política de Seguridad de las Tecnologías de la Información y la Comunicación en el Servicio Aragonés de Salud y se crean el Comité de Seguridad de la Información y la figura del Responsable de Seguridad.

El desarrollo y el impulso de la Sociedad de la Información y la aplicación de las tecnologías en los campos de la informática y las telecomunicaciones, son ya un hecho consolidado, que afecta tanto a la sociedad como a los poderes públicos, siendo éstos los responsables de generar confianza en el uso global por parte de la ciudadanía de los medios tecnológicos en sus relaciones con la Administración Pública. Para ello, dichos medios deben ser seguros, garantizando la confidencialidad, integridad y disponibilidad de la información y de los servicios telemáticos en los que se apoya, permitiendo tanto a la ciudadanía como a las Administraciones Públicas, el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.

En este sentido, la Ley Orgánica 5/2007, de 20 de abril, de reforma del Estatuto de Autonomía de Aragón, en su artículo 28.2, establece que los poderes públicos deberán promover las condiciones que garanticen en el territorio de Aragón el acceso sin discriminaciones a los servicios audiovisuales y a las tecnologías de la información y la comunicación.

La Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, señala entre sus fines el crear las condiciones de confianza en el uso de los medios electrónicos, estableciendo las medidas necesarias para la preservación de la integridad de los derechos fundamentales, y en especial los relacionados con la intimidad y la protección de datos de carácter personal, por medio de la garantía de la seguridad de los sistemas, los datos, las comunicaciones y los servicios electrónicos.

Del mismo modo, la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, así como su Reglamento de Desarrollo 1720/2007, aportan criterios para establecer la proporcionalidad entre las medidas de seguridad y la información a proteger, información que en el caso del Servicio Aragonés de Salud es en su mayor parte de nivel alto, según la citada ley orgánica, siendo por ello mayor el celo y la necesidad de implementar cuantas medidas sean necesarias para garantizar la confidencialidad, disponibilidad e integridad de la información.

Estos fines han sido definidos y desarrollados 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. Es precisamente en esta norma donde, en su artículo 11, se establece que todos los órganos superiores de las Administraciones Públicas deberán contar con una Política de Seguridad, así como con un comité de seguridad de la información y un responsable de seguridad.A estos efectos, conforme a lo establecido en el mismo artículo, se consideran órganos superiores, los responsables directos de la ejecución de la acción del gobierno, central, autonómico o local, en un sector de actividad específico.

Por otra parte, de acuerdo con el Decreto Legislativo 2/2004, de 30 de diciembre, del Gobierno de Aragón, por el que se aprueba el texto refundido de la Ley del Servicio Aragonés de Salud, el Servicio Aragonés de Salud se configura como un organismo autónomo, que adscrito al Departamento responsable en materia de Salud de la Administración de la Comunidad Autónoma, está dotado de personalidad jurídica propia y plena capacidad de obrar, patrimonio propio y recursos humanos, financieros y materiales, al objeto de hacer efectivo el derecho a la protección de la salud en el ámbito de la Comunidad Autónoma, de acuerdo con lo establecido en los artículos 43 y concordantes de la Constitución Española.

En consecuencia con todo lo expuesto, la presente orden viene a establecer el compromiso del Servicio Aragonés de Salud con la seguridad de los sistemas de información, y dar cumplimiento a las disposiciones del Esquema Nacional de Seguridad, definiendo así los objetivos y criterios básicos para el tratamiento de la misma, y sentando los pilares del marco normativo de seguridad del Servicio Aragonés de Salud, concretados en el Comité de Seguridad de la Información, y en la figura del Responsable de Seguridad. De este modo, la presente orden, aprueba y da a conocer la Política de Seguridad de las Tecnologías de la Información y la Comunicación del servicio Aragonés de Salud, sus objetivos y principios básicos, el marco de referencia común y la descripción de la estructura organizativa sobre la que se apoyará el gobierno de la seguridad en el Servicio Aragonés de Salud.

Por todo ello, y en virtud de las competencias previstas en el Decreto 337/2011, de 6 de octubre, del Gobierno de Aragón, por el que se aprueba la estructura orgánica del Departa-

csv: BOA20150414008

mento de Sanidad, Bienestar Social y Familia, y en el artículo 43.4 de la Ley 2/2009, de 11 de mayo, del Presidente y del Gobierno de Aragón, dispongo:

Artículo primero.— *Política de Seguridad de la Información.*

Se aprueba la Política de Seguridad de las Tecnologías de la Información y la Comunicación (en adelante Política de Seguridad TIC), del Servicio Aragonés de Salud, recogida en el anexo, que se ha de aplicar en el tratamiento de los activos TIC de su titularidad o cuya gestión tenga encomendada, conformando, junto a la normativa que la desarrolle, el marco normativo de seguridad TIC del Servicio Aragonés de Salud, sin perjuicio de las directrices establecidas o que puedan establecerse por otros órganos competentes en materia de sistemas de información del Gobierno de Aragón.

Artículo segundo.— *Definiciones y estándares.*

A los efectos previstos en esta resolución, las definiciones y estándares han de ser entendidas en el sentido indicado en el Esquema Nacional de Seguridad.

Disposición final única.— *Entrada en vigor.*

La presente orden entrará en vigor el día siguiente al de su publicación en el "Boletín Oficial de Aragón".

Zaragoza, 16 de marzo de 2015.

El Consejero de Sanidad, Bienestar Social y Familia,
RICARDO OLIVÁN BELLOSTA

csv: BOA20150414008

A N E X O

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DEL SERVICIO ARAGONÉS DE SALUD

1. Misión del Servicio Aragonés de Salud.

El DECRETO LEGISLATIVO 2/2004, de 30 de diciembre, del Gobierno de Aragón, por el que se aprueba el Texto Refundido de la Ley del Servicio Aragonés de Salud, establece los objetivos básicos del Servicio Aragonés de Salud:

a) La atención integral de la salud individual y comunitaria de la población aragonesa, mediante la prestación de los servicios sanitarios, en condiciones de igualdad para toda la población.

b) El aprovechamiento óptimo de los recursos sanitarios disponibles, con el fin de elevar el nivel de salud en la comunidad.

c) Promover la distribución equitativa de los servicios sanitarios, tendente a superar los desequilibrios territoriales y sociales en el ámbito de la Comunidad Autónoma.

d) La coordinación funcional de las actividades de las instituciones públicas y privadas, mediante el establecimiento de convenios, conciertos o cualesquiera otras fórmulas de gestión o titularidad compartida, que permita alcanzar el máximo rendimiento de los recursos disponibles y garantizar al máximo la cantidad y calidad de la asistencia sanitaria

2. Marco legal.

El marco legal en el que el Servicio Aragonés de Salud está constituido por el conjunto de leyes y normas, tanto de ámbito nacional, como autonómico, desarrollan los principios constitucionales en relación a la protección de la salud.

Las normas más destacadas son:

- LEY ORGÁNICA 5/2007, de 20 de abril de reforma del Estatuto de Autonomía de Aragón. Establece en su artículo 14, sobre el derecho a la salud, que:

  1. Todas las personas tienen derecho a acceder a los servicios públicos de salud, en condiciones de igualdad, universalidad y calidad, y los usuarios del sistema público de salud tienen derecho a la libre elección de médico y centro sanitario, en los términos que establecen las leyes.

  2. Los poderes públicos aragoneses garantizarán la existencia de un sistema sanitario público desarrollado desde los principios de universalidad y calidad, y una asistencia sanitaria digna, con

csv: BOA20150414008

información suficiente al paciente sobre los derechos que le asisten como usuario.

- LEY 6/2002, de 15 de abril, de Salud de Aragón, que tiene por objeto:
  1. La regulación general de todas las acciones que permitan hacer efectivo el derecho a la protección de la salud reconocido en los artículos 43 y concordantes de la Constitución.
  2. La ordenación del Sistema de Salud de Aragón, en el que se integra y articula funcionalmente el conjunto de actividades, servicios y prestaciones que tienen por finalidad la promoción y protección de la salud, la prevención de la enfermedad y la asistencia sanitaria en los casos de pérdida de la salud, además de las acciones rehabilitadoras oportunas.
- DECRETO LEGISLATIVO 2/2004, de 30 de diciembre, del Gobierno de Aragón, por el que se aprueba el Texto Refundido de la Ley del Servicio Aragonés de Salud. Establece y desarrolla los objetivos y principios del Servicio Aragonés de Salud.

3.- Objetivos de la Política de Seguridad TIC.

El uso extensivo de tecnologías de la información en el Servicio Aragonés de Salud, hace necesario definir una Política de Seguridad de la Información, con el objetivo de establecer directrices básicas y duraderas para una protección eficaz de la información.

La presente Política de Seguridad de la Información constituye el marco de referencia para establecer el Sistema de Gestión de la Seguridad de la Información (SGSI) del Servicio Aragonés de Salud. El enfoque para la gestión de la seguridad adoptado en el SGSI se basará en el recomendado por la norma ISO/IEC27001 (Tecnología de la información-Técnicas de seguridad-Sistemas de Gestión de la Seguridad de la Información (SGSI)-Requisitos). Las directrices recogidas en este documento han sido elegidas de acuerdo con el estándar ISO/IEC 27002 («Código de buenas prácticas para la Gestión de la Seguridad de la Información»), que establece un marco de referencia de seguridad respaldado y reconocido internacionalmente. Este marco tecnológico, organizativo y procedimental de seguridad se soporta en un conjunto de normas, estándares, procedimientos y herramientas de seguridad para la protección de la información, entre ellos la metodología MAGERIT de análisis y gestión de riesgos.

La aprobación de esta política manifiesta el interés del Servicio Aragonés de Salud en la gestión de la seguridad de la información y en la mejora continua del SGSI. Con ella se establecen los objetivos y las responsabilidades necesarias para proteger los activos de información, garantizando la integridad, disponibilidad y confidencialidad de los mismos, cumpliendo con el marco legal vigente y respetando las directrices, normas y procedimientos que

csv: BOA20150414008

oportunamente se establezcan. La política de seguridad TIC del Servicio Aragonés de Salud, persigue la consecución de los siguientes objetivos:

a) Garantizar a toda la ciudadanía aragonesa que sus datos serán gestionados de acuerdo a los estándares y buenas prácticas en seguridad TIC.

b) Aumentar el nivel de concienciación y la confianza en materia de seguridad TIC en el Servicio Aragonés de Salud, garantizando que el personal es consciente de sus obligaciones y responsabilidades.

c) Establecer las bases de un modelo integral de gestión de la seguridad TIC en el Servicio Aragonés de Salud, que cubra en un ciclo continuo de mejora los aspectos técnicos, organizativos y procedimentales.

d) Garantizar el cumplimiento de la legislación vigente en materia de seguridad TIC.

e) Reducir el riesgo de posibles contingencias, reaccionando ante cualquier tipo de incidencia que se produzca en materia de seguridad TIC.

***4.-* Principios de la Política de Seguridad TIC.**

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

a. Principio de seguridad integral 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.

   Se prestará la máxima atención a la concienciación de las personas que intervienen en el proceso y a sus responsables jerárquicos, para que, ni la ignorancia, ni la falta de organización y coordinación, ni instrucciones inadecuadas, sean fuentes de riesgo para la seguridad

b. Principio de gestión de riesgos.

   Se articulará 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.

   La gestión de riesgos permitirá el mantenimiento de un entrono 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, los riesgos a los que estén expuestos y las medidas de seguridad.

c. Principio de prevención, reacción y recuperación.

csv: BOA20150414008

- La seguridad del sistema debe contemplar los aspectos de prevención, detección y corrección, para conseguir que las amenazas sobre el mismo no se materialicen, no afecten gravemente a la información que maneja, o los servicios que se prestan.
- Las medidas de prevención deben eliminar o, al menos reducir, la posibilidad de que las amenazas lleguen a materializarse con perjuicio para el sistema. Estas medidas de prevención contemplarán, entre otras, la disuasión y la reducción de la exposición.
- Las medidas de detección estarán acompañadas de medidas de reacción, de forma que los incidentes de seguridad se atajen a tiempo.
- Las medidas de recuperación permitirán la restauración de la información y los servicios, de forma que se pueda hacer frente a las situaciones en las que un incidente de seguridad inhabilite los medios habituales.
- Sin merma de los demás principios básicos y requisitos mínimos establecidos, el sistema garantizará la conservación de los datos e informaciones en soporte electrónico.

  De igual modo, el sistema mantendrá disponibles los servicios durante todo el ciclo vital de la información digital, a través de una concepción y procedimientos que sean la base para la preservación del patrimonio digital.

d. Principio de líneas de defensa.

- El sistema ha de disponer de una estrategia de protección constituida por múltiples capas de seguridad, dispuesta de forma que, cuando una de las capas falle, permita:
  - Ganar tiempo para una reacción adecuada frente a los incidentes que no han podido evitarse.
  - Reducir la probabilidad de que el sistema sea comprometido en su conjunto.
  - Minimizar el impacto final sobre el mismo.
- Las líneas de defensa han de estar constituidas por medidas de naturaleza organizativa, física y lógica.

e. Principio de reevaluación periódica.

Las medidas de seguridad se reevaluarán y actualizarán periódicamente, para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección, llegando incluso a un replanteamiento de la seguridad, si fuese necesario.

csv: BOA20150414008

f. 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 la información tratada; el responsable del servicio 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.

La responsabilidad de la seguridad de los sistemas de información estará diferenciada de la responsabilidad sobre la prestación de los servicios.

La política de seguridad de la organización detallará las atribuciones de cada responsable y los mecanismos de coordinación y resolución de conflictos.

***5.-* Requisitos de la Política de Seguridad TIC.**

La política de seguridad TIC del Servicio Aragonés de Salud se establecerá en base a los principios básicos indicados y se desarrollará aplicando los siguientes requisitos mínimos:

Todos estos requisitos mínimos se exigirán con un enfoque de proporcionalidad en los costes económicos y operativos en base a los riesgos identificados en cada sistema, pudiendo algunos no requerirse en sistemas sin riesgos significativos, y se cumplirán de acuerdo con lo establecido en el artículo 27 del Esquema Nacional de Seguridad.

a) Organización e implantación del proceso de seguridad.

La seguridad compromete a todos los miembros de la organización. La preservación de la seguridad TIC será considerada objetivo común de todos los empleados del Servicio Aragonés de Salud, siendo éstos responsables del uso correcto de los activos TIC puestos a su disposición.

Los responsables de cada unidad deberán velar por el cumplimiento de la política de seguridad que deberá ser conocida por todos los miembros de la organización.

b) Análisis y gestión de los riesgos.

- Cada unidad que desarrolle e implante sistemas para el tratamiento de la información y las comunicaciones realizará su propia gestión de riesgos.
- Esta gestión se realizará por medio del análisis y tratamiento de los riesgos a los que está expuesto el sistema. A estos efectos, se empleará alguna metodología reconocida internacionalmente.

csv: BOA20150414008

- Las medidas adoptadas para mitigar o suprimir los riesgos deberán estar justificadas y, en todo caso, existirá una proporcionalidad entre ellas y los riesgos.

c) Gestión de personal.

- Todo el personal relacionado con la información y los sistemas deberá ser formado e informado de sus deberes y obligaciones en materia de seguridad. Sus actuaciones deben ser supervisadas para verificar que se siguen los procedimientos establecidos.
- El personal relacionado con la información y los sistemas, ejercitará y aplicará los principios de seguridad en el desempeño de su cometido.
- El significado y alcance del uso seguro del sistema se concretará y plasmará en unas normas de seguridad.
- Para corregir, o exigir responsabilidades en su caso, cada usuario que acceda a la información del sistema debe estar identificado de forma única, de modo que se sepa, en todo momento, quién recibe derechos de acceso, de qué tipo son éstos, y quién ha realizado determinada actividad.

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: instalación, mantenimiento, gestión de incidencias y desmantelamiento.
- El personal de cada unidad del Servicio Aragonés de Salud recibirá la formación específica necesaria para garantizar la seguridad de las tecnologías de la información aplicables a los sistemas y servicios de la organización.
- Las unidades del Servicio Aragonés de Salud exigirán, de manera objetiva y no discriminatoria, que las organizaciones que les presten servicios de seguridad cuenten con unos niveles idóneos de gestión y madurez en los servicios prestados.

e) Autorización y control de los accesos.

El acceso al sistema de información deberá ser controlado y limitado a los usuarios, procesos, dispositivos y otros sistemas de información, debidamente autorizados, restringiendo el acceso a las funciones permitidas.

f) Protección de las instalaciones.

Los sistemas se instalarán en áreas separadas, dotadas de un procedimiento de control de acceso. Como mínimo, las salas deben estar cerradas y disponer de un control de llaves.

g) Adquisición de productos de seguridad.

csv: BOA20150414008

- En la adquisición de productos de seguridad de las tecnologías de la información y comunicaciones que vayan a ser utilizados por el Servicio Aragonés de Salud se valorarán positivamente aquellos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición.
- La certificación indicada en el apartado anterior deberá estar de acuerdo con las normas y estándares de mayor reconocimiento internacional, en el ámbito de la seguridad funcional.

h) Seguridad por defecto.

Los sistemas deben diseñarse y configurarse de forma que garanticen la seguridad por defecto:

- El sistema proporcionará la mínima funcionalidad requerida para que la organización sólo alcance sus objetivos, y no alcance ninguna otra funcionalidad adicional.
- Las funciones de operación, administración y registro de actividad serán las mínimas necesarias, y se asegurará que sólo son accesibles por las personas, o desde emplazamientos o equipos, autorizados, pudiendo exigirse en su caso restricciones de horario y puntos de acceso facultados.
- En un sistema de explotación se eliminarán o desactivarán, mediante el control de la configuración, las funciones que no sean de interés, sean innecesarias e, incluso, aquellas que sean inadecuadas al fin que se persigue.
- El uso ordinario del sistema ha de ser sencillo y seguro, de forma que una utilización insegura requiera de un acto consciente por parte del usuario.

i) Integridad y actualización del sistema.

- Todo elemento físico o lógico requerirá autorización formal previa a su instalación en el sistema.
- Se deberá conocer en todo momento el estado de seguridad de los sistemas, en relación a las especificaciones de los fabricantes, a las vulnerabilidades y a las actualizaciones que les afecten, reaccionando con diligencia para gestionar el riesgo a la vista del estado de seguridad de los mismos.

j) Protección de información almacenada y en tránsito.

- En la estructura y organización de la seguridad del sistema, se prestará especial atención a la información almacenada o en tránsito a través de entornos inseguros. Tendrán la consideración de entornos inseguros los equipos portátiles, asistentes personales (PDA), dispositivos periféricos, soportes de información y comunicaciones sobre redes abiertas o con cifrado débil.

csv: BOA20150414008

- Forman parte de la seguridad los procedimientos que aseguren la recuperación y conservación a largo plazo de los documentos electrónicos producidos por el Servicio Aragonés de Salud en el ámbito de sus competencias.
- Toda información en soporte no electrónico, que haya sido causa o consecuencia directa de la información electrónica, deberá estar protegida con el mismo grado de seguridad que ésta. Para ello se aplicarán las medidas que correspondan a la naturaleza del soporte en que se encuentren, de conformidad con las normas de aplicación a la seguridad de los mismos.

k) Prevención ante otros sistemas de información interconectados.

El sistema ha de proteger el perímetro, en particular, si se conecta a redes públicas. Se entenderá por red pública de comunicaciones la red de comunicaciones electrónicas que se utiliza, en su totalidad o principalmente, para la prestación de servicios de comunicaciones electrónicas disponibles para el público, de conformidad a la definición establecida en el apartado 26 del anexo II, de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones. En todo caso se analizarán los riesgos derivados de la interconexión del sistema, a través de redes, con otros sistemas, y se controlará su punto de unión.

l) Registro de actividad.

Con la finalidad exclusiva de lograr el cumplimiento de la Política de Seguridad del SALUD y de la normativa aplicable, con plenas garantías del derecho al honor, a la intimidad personal y familiar y a la propia imagen de los afectados, y de acuerdo con la normativa sobre protección de datos personales, de función pública o laboral, y demás disposiciones que resulten de aplicación, 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 establecerá un sistema de detección y reacción frente a código dañino.
- Se registrarán los incidentes de seguridad que se produzcan y las acciones de tratamiento que se sigan. Estos registros se emplearán para la mejora continua de la seguridad del sistema.

n) Continuidad de la actividad.

Los sistemas dispondrán de copias de seguridad y establecerán los mecanismos necesarios para garantizar la continuidad de las operaciones, en caso de pérdida de los medios habituales de trabajo.

csv: BOA20150414008

o) Mejora continua del proceso de seguridad.

El proceso integral de seguridad implantado deberá ser actualizado y mejorado de forma continua. Para ello, se aplicarán los criterios y métodos reconocidos en la práctica nacional e internacional relativos a gestión de las tecnologías de la información.

6.- Cumplimiento de requisitos mínimos.

Para dar cumplimiento a los requisitos mínimos anteriores se aplicarán las medidas de seguridad correspondientes, teniendo en cuenta:

- Los activos que constituyen el sistema.
- La categoría del sistema, según lo previsto en el Esquema Nacional de Seguridad.
- Las decisiones que se adopten para gestionar los riesgos identificados.

Cuando un sistema al que afecte maneje datos de carácter personal le será de aplicación lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, y normativa de desarrollo, sin perjuicio de los requisitos establecidos en el Esquema Nacional de Seguridad.

Los medidas a las que se refieren los apartados anteriores tendrán la condición de mínimos exigibles, y podrán ser ampliados por causa de la concurrencia indicada o del prudente arbitrio del responsable de la información, habida cuenta del estado de la tecnología, la naturaleza de los servicios prestados y la información manejada, y los riesgos a que están expuestos.

7. Ámbito de aplicación.

El alcance de la política de seguridad incluye a todos los hospitales, centros de salud, centros de salud mental, consultorios, centros de atención especializada, centros de atención sociosanitaria, puntos de atención continuada, servicios de urgencia de atención primaria, 061 y centros directivos y de administración del Servicio Aragonés de Salud en la Comunidad Autónoma de Aragón en los que los empleados acceden a los sistemas de información del Servicio Aragonés de Salud, así como las empresas proveedoras de servicios relacionados.

La política de seguridad es aplicable a todos los sistemas de información del Servicio Aragonés de Salud y/o que den soporte a sus procesos y afecta a todos los activos de información sustentados en ellos. La política de seguridad se encuentra enmarcada en el sistema de gestión de la seguridad de la información (SGSI) del Servicio Aragonés de Salud.

csv: BOA20150414008

8. Normativa de seguridad.

El sistema de gestión de la seguridad de la información (SGSI) queda formalmente establecido mediante una normativa de seguridad, formada por la presente política y las normas, estándares y procedimientos operativos que la desarrollan. El Responsable de seguridad se encargará de la gestión de los documentos de la normativa, debiendo asegurar que ésta sea completa y proporcione información suficiente para definir las necesidades de protección de la información y los activos asociados a la misma en el ámbito del Servicio Aragonés de Salud. Los documentos de la normativa de seguridad serán publicados y divulgados con el objetivo de que sean conocidos y aplicados por todos los usuarios afectados.

9. Organización y gestión de la seguridad.

9.1. Responsabilidad general.

Todos y cada uno de los usuarios de los sistemas de información del Servicio Aragonés de Salud son responsables de la seguridad de los activos TIC mediante un uso correcto de los mismos, siempre de acuerdo con sus atribuciones profesionales.

9.2. Responsabilidad específica.

La gestión de los procesos de seguridad recogidos en el SGSI del Servicio Aragonés de Salud es responsabilidad de un conjunto de personas con funciones concretas, definidas y documentadas. El personal que desempeñe tareas específicas relacionadas con seguridad de la información recibirá la formación adecuada que se ajuste a sus funciones y nivel de responsabilidad. Para una mejor respuesta ante incidentes de seguridad, el Servicio Aragonés de Salud mantendrá relaciones de cooperación en materia de seguridad con las autoridades competentes, 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. Responsable de Seguridad TIC del Servicio Aragonés de Salud.

Al frente de la gestión de la seguridad de la información habrá una persona responsable de la misma.

El Responsable de Seguridad TIC, será designado por la Dirección Gerencia del Salud, entre profesionales de la misma.

En su caso, el Responsable de Seguridad de la Información podrá compatibilizar este cargo con las funciones propias de su puesto de trabajo.

Al Responsable de Seguridad le corresponden las siguientes funciones:

csv: BOA20150414008

a) Proponer, coordinar, informar, gestionar los incidentes y hacer seguimiento de las actuaciones relacionadas con la seguridad TIC de los activos de información del Servicio Aragonés de Salud, así como la realización de las auditorías periódicas que correspondan.

b) Asesorar y dar soporte al Comité de Seguridad de la Información en materia de Seguridad TIC en el Servicio Aragonés de Salud, elevando propuestas e informes y elaborando los procedimientos que sean necesarios.

c) Asumir las funciones en el Servicio Aragonés de Salud atribuidas al Responsable de Seguridad 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 y resto de normativa vigente en la materia.

d) Coordinarse con los servicios informáticos del Servicio Aragonés de Salud, del Departamento de Sanidad, Bienestar Social y Familia y los servicios corporativos del Gobierno de Aragón, tanto en materia de sistemas de información en general, como de seguridad de la información en particular.

e) Canalizar la relación con el Servicio competente en materia de seguridad de la información, legalización de ficheros, y tramitación de su registro ante el órgano competente en materia de protección de datos de la Comunidad Autónoma de Aragón

f) Proponer la inclusión, adecuación y clasificación de Sistemas de Información que forman parte del Inventario de activos de Información del Servicio Aragonés de Salud, especialmente los relativos a la Historia Clínica Electrónica y a los ficheros con datos de carácter personal declarados, así como evaluar y gestionar los riesgos que atañen a los mismos para determinar el impacto de las amenazas. No obstante, establecer las valoraciones respecto a la categoría de cada sistema de información serán atribuidas a los responsables de cada sistema de información ó servicio, según designa el artículo 44 del RD 3/2010.

g) Implantar criterios comunes para la correcta gestión de los derechos de acceso, rectificación, cancelación y oposición y la conservación y destrucción de documentos que contempla la LOPD, sobre la Historia Clínica Electrónica y los ficheros con datos de carácter personal declarados responsabilidad de la Dirección Gerencia del Servicio Aragonés de Salud gestionando y resolviendo cualquier cuestión relacionada que le sea planteada, teniendo en cuenta siempre los criterios y directrices establecidos por el Servicio de Administración Electrónica de la Dirección General de Función Pública y Calidad de los Servicios, órgano competente en materia de protección de datos de la Diputación General de Aragón

h) Elaborar propuestas de actividades formativas e informativas dirigidas a profesionales sobre el uso seguro de los Sistemas de Información y a

csv: BOA20150414008

profesionales y pacientes sobre el uso seguro de la Historia Clínica Electrónica, promoviendo de esa forma la cultura de la Seguridad de la Información y la concienciación en esa materia de los profesionales del Servicio Aragonés de Salud.

i) Establecer los mecanismos de coordinación necesarios con las diferentes Comisiones de Historias Clínicas existentes en los Sectores Sanitarios del Servicio Aragonés de Salud.

11.- Comité de Seguridad de la Información del Servicio Aragonés de Salud.

Se crea el Comité de Seguridad de la Información del Servicio Aragonés de Salud, así como la creación de la figura del Responsable de Seguridad, que formará parte del citado Comité.

El Comité de Seguridad de la Información es un órgano adscrito a la Dirección Gerencia del Servicio Aragonés de Salud, de carácter científico técnico, cuya misión es elaborar propuestas y documentos de trabajo en relación con las funciones encomendadas, así como analizar su viabilidad técnica y económica y llevar a cabo la ejecución de aquellas actuaciones que así se determinen.

La designación y cese de los miembros del Comité se efectuará mediante resolución de la Dirección Gerencia del Servicio Aragonés de Salud.

El Comité de Seguridad de la Información, en lo regulado en la presente Orden, se regirá por lo dispuesto para los órganos colegiados en el Titulo II, Capítulo II de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

12.- Composición del Comité de Seguridad de la Información

El Comité se compondrá de un mínimo de 5 y hasta un máximo de 15 miembros, entre los cuales estarán incluidos, presidente y secretario y vocales, designados todos ellos por la Dirección Gerencia del Servicio Aragonés de Salud entre personal facultativo y de enfermería, así como expertos en los diversos campos que atañen a la documentación clínica electrónica (informáticos, ingenieros, abogados etc.…), de los distintos sectores sanitarios, tanto de Atención Primaria como Especializada y de Servicios Centrales. Uno de ellos deberá ser el Responsable de Seguridad TIC del Servicio Aragonés de Salud.

El presidente y el secretario del Comité serán designados por la Dirección Gerencia del Servicio Aragonés de Salud. En caso de vacante ausencia o enfermedad, serán sustituidos por el miembro del órgano de mayor y menor jerarquía, antigüedad y edad, por este orden, respectivamente.

La pertenencia del resto de los miembros del Comité tendrá carácter personal, sin que puedan ser sustituidos en caso de vacante, ausencia o enfermedad.

csv: BOA20150414008

Con carácter excepcional podrá ampliarse la composición del Comité a criterio de la Dirección Gerencia.

Podrán crearse grupos de trabajo, dentro del Comité, caso de ser entenderse necesarios.

El Comité podrá invitar a participar en sus discusiones a todos aquellos profesionales que considere oportuno, quienes 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.

13.- Funciones del Comité de Seguridad de la Información.

Corresponde al Comité de Seguridad de la Información del Servicio Aragonés de Salud ser el órgano de gestión y coordinación de la Dirección Gerencia del Servicio Aragonés de Salud, en relación a la toma de decisiones sobre la seguridad, normalización, gestión y mejora de los Sistemas de Información del Servicio Aragonés de Salud, así como velar por el cumplimiento de los derechos de acceso, rectificación, cancelación y oposición de los ciudadanos en relación con la misma.

Concretamente, se atribuyen al Comité las siguientes funciones:

a) Velar por la actualización y vigencia de la Política de Seguridad TIC, supervisando en todo momento el cumplimiento de la normativa de protección de datos y seguridad de la información.

b) Aprobar y realizar el seguimiento de objetivos, iniciativas y planes estratégicos en materia de seguridad de la información.

c) Elevar propuestas de revisión del marco normativo de seguridad de la información al órgano competente para su reglamentaria tramitación, asegurando el alineamiento de las actuaciones de seguridad con las iniciativas, políticas y proyectos corporativos del Gobierno de Aragón, así como con la Comisión Interdepartamental de Administración Electrónica del Gobierno de Aragón.

d) Analizar el registro de gestión de incidencias y elaborar propuestas en el uso seguro de la Información.

14.- Funciones del Presidente, Secretario y Vocales del Comité.

Al presidente del Comité le corresponden las siguientes funciones:

a) Ostentar, a todos los efectos, la representación del Comité.

b) Acordar la convocatoria de las sesiones ordinarias y extraordinarias y elaborar el orden del día, en colaboración con el Secretario y teniendo en cuenta, en su caso, las peticiones de los demás miembros que hayan sido formuladas con una antelación mínima de siete días.

csv: BOA20150414008

c) Presidir las sesiones del Comité, tanto ordinarias como extraordinarias, moderar el desarrollo de los debates y suspenderlos por causas justificadas.

d) Coordinar las actividades del Comité y proponer grupos de trabajo si fuera preciso.

e) Visar las actas y certificaciones de los acuerdos de las Comisiones.

f) Presentar a la Dirección Gerencia del Servicio Aragonés de Salud los documentos e informes elaborados.

g) Dirimir con su voto los empates, a efectos de adoptar acuerdos.

Al Secretario del Comité le corresponden las siguientes funciones:

a) Asistir a las reuniones con voz y voto.

b) Efectuar las convocatorias del Comité por orden de su Presidente, así como las citaciones a los miembros de la misma.

c) Recibir los actos de comunicación de los miembros con el Comité y, por tanto, las notificaciones, peticiones de datos, rectificaciones o cualquier otro escrito de los que deba tener conocimiento.

d) Elaborar las actas de las reuniones del Comité.

e) Supervisar las labores de la secretaría administrativa de el Comité: correo, archivo y documentos (informes, programas, recomendaciones, protocolos, etc.…).

f) Expedir certificaciones de las consultas, dictámenes o acuerdos aprobados en el Comité.

g) Colaborar con el Presidente en las labores de coordinación y elaboración de los órdenes del día.

A los vocales del Comité les corresponden las siguientes funciones:

a) Colaborar con el Presidente y el Secretario en todas aquellas actividades de coordinación que se deriven del trabajo del Comité.

b) Tener una participación activa en los trabajos del Comité.

c) Comunicar a el Comité cuantos hechos, circunstancias o aspectos relacionados con los cometidos de la misma conozcan en el desarrollo de la actividad cotidiana.

d) Participar en la definición del planteamiento técnico y operativo de los objetivos, iniciativas y planes estratégicos de seguridad de la Información, así como en la elaboración de propuestas relativas a la revisión del marco normativo de seguridad TIC.

e) Elaborar los informes y propuestas en materia de seguridad TIC del Servicio Aragonés de Salud que se le encomienden por el Presidente de la Comisión.

csv: BOA20150414008

15.- Convocatorias y sesiones del Comité de Seguridad de la Información..

El Comité establecerá un calendario mínimo de dos reuniones al año.

El Comité se reunirá, cuantas veces lo acuerde su Presidente, la Dirección Gerencia del Servicio Aragonés de Salud o el 25% de sus miembros. El Comité nombrará entre sus miembros un grupo de respuesta a incidentes TIC cuya función será la toma urgente de decisiones en caso de contingencia grave que afecte a la seguridad de sistemas de información críticos del Servicio Aragonés de Salud.

Para la válida constitución del órgano, a efectos de celebración de sesiones, deliberaciones y toma de acuerdos, se requerirá la presencia del Presidente y Secretario o, en su caso, de quienes le sustituyan, y la de la mitad más uno de sus miembros.

Los acuerdos del Comité serán adoptados por mayoría de votos.

16. Clasificación y Control de Activos.

Los activos TIC del Servicio Aragonés de Salud se encontrarán inventariados, con un responsable asociado y, en caso de ser necesario, un custodio de los mismos. Los inventarios se mantendrán actualizados para asegurar su validez. Los activos de información estarán clasificados de acuerdo a su sensibilidad y criticidad para el desarrollo de la actividad del Servicio Aragonés de Salud, en función de la cual se establecerán las medidas de seguridad exigidas para su protección.

17. Seguridad física y ambiental.

Los sistemas de información serán emplazados en áreas seguras protegidas con controles de acceso físicos adecuados al nivel de criticidad de los mismos. Los sistemas y la información que soportan estarán adecuadamente protegidos frente a amenazas físicas o ambientales, sean éstas intencionadas o accidentales.

18. Gestión de sistemas, operaciones y comunicaciones.

El Servicio Aragonés de Salud asegurará la correcta gestión y operación de los sistemas de información estableciendo estándares de seguridad y adoptando las mejores prácticas en materia de seguridad (configuración, mecanismos de protección, actualización, monitorización, detección de vulnerabilidades, respaldo de información, etc.).

csv: BOA20150414008

Las incidencias relacionadas con seguridad de la información serán registradas, notificadas y resueltas a la mayor brevedad posible por el personal asignado para ello.

Los entornos de desarrollo y pruebas estarán separados en la medida de lo posible y serán independientes de los entornos productivos con el fin de mantener la seguridad de los datos reales de producción y el rendimiento de los servicios. Toda información que se transmita a través de redes de comunicaciones deberá ser adecuadamente protegida mediante mecanismos que garanticen su seguridad. El almacenamiento, manipulación, transporte, destrucción o desecho de cualquier activo que soporte información del Servicio Aragonés de Salud garantizará la imposibilidad de acceso o recuperación de su contenido por parte de personal no autorizado.

19. Control de acceso.

El Servicio Aragonés de Salud pone a disposición de sus usuarios la capacidad de acceder a sus sistemas de información y visualizar o modificar la información que procesan y almacenan. Los permisos de acceso a las redes, sistemas y a la propia información serán otorgados mediante un proceso formal de aprobación que asegure que los usuarios tengan acceso únicamente a los recursos e información necesarios para el desempeño de sus funciones en el Servicio Aragonés de Salud.

Todos los empleados y personal externo, así como entidades colaboradoras que accedan a los sistemas de información del Servicio Aragonés de Salud, quedarán registrados y dispondrán de credenciales personales e intransferibles.

Toda persona registrada que disponga de credenciales de acceso será responsable de mantener la confidencialidad y asegurar su correcto uso, especialmente si el acceso es a la Historia Clínica Electrónica.

20. Desarrollo y mantenimiento de sistemas.

Las aplicaciones que se desarrollen para el Servicio Aragonés de Salud deberán contemplar aspectos de seguridad de la información en todas las fases del ciclo de vida de desarrollo, desde la toma de requisitos hasta la realización de pruebas y el paso a producción.

21. Gestión de continuidad de actividad.

El Servicio Aragonés de Salud dispondrá de un plan para mantener la continuidad de los procesos y sistemas críticos y garantizar su recuperación en caso de desastre. La finalidad de este plan es reducir el tiempo de indisponibilidad a niveles aceptables mediante la combinación de controles

csv: BOA20150414008

de carácter organizativo, tecnológico y procedimental tanto preventivos como de recuperación.

22. Conformidad.

El Servicio Aragonés de Salud adoptará las medidas técnicas y organizativas necesarias para mantener sus sistemas de información adaptados a la normativa legal vigente, y especialmente a aquellas regulaciones legales relativas al tratamiento de los datos de carácter personal.

Es responsabilidad de todos los empleados conocer y cumplir la legislación vigente de aplicación en sus ámbitos de actuación. Las contrataciones y acuerdos de nivel de servicios que se establezcan con terceros incluirán cláusulas y garantías de cumplimiento de los requisitos de seguridad que exija el Servicio Aragonés de Salud y la normativa legal vigente. Con carácter periódico se realizarán auditorías que comprueben el grado de conformidad con la política y la legislación, y revisiones que determinen el grado de cumplimiento de los objetivos de seguridad establecidos y la eficacia de los controles establecidos. Los resultados obtenidos determinarán las líneas de actuación a seguir y las posibles modificaciones a realizar sobre los controles y la normativa de seguridad.

csv: BOA20150414008