Aragonesa de Servicios Telemáticos

ARAGONESA DE SERVICIOS TELEMÁTICOS

Política de Seguridad de Aragonesa de Servicios Telemáticos

Referencia:	POL_SeguridadInformacion.docx
Autor:	Área de Seguridad
Fecha de creación:	09/03/2018
Última actualización:	09/03/2018
Versión:	v1.1
Clasificación:	Uso Publico

GOBIERNO DE ARAGON
Departamento de Innovación, Investigación y Universidad

Control del documento

Registro de cambios

Versión	Fecha	Autor	Descripción
0.8	22/05/2012	Área de Seguridad	Revisión del Comité de Seguridad TIC de AST
0.9	15/11/2017	Área de Seguridad	Adecuación ENS
1.0	21/12/2017	Área de seguridad	Aprobación Comité de Seguridad TIC de AST
1.1	08/03/2018	Área de Seguridad	Revisiones menores de formato y estilo

Revisores

Nombre	
Comité de Seguridad TIC de AST	Mayte Ortín, Nieves Campillo, Fidel Contreras, Óscar Torrero, Jordi Dalmau, David López

Lista de distribución

Nombre	Área
Comité de Seguridad TIC de AST	Mayte Ortín (presidenta), Nieves Campillo, Fidel Contreras, Óscar Torrero, Jordi Dalmau, David López (secretario)

Entidad Pública Aragonesa de Servicios Telemáticos
Av Pablo Ruiz Picasso, 63 A 3ª J • 50018 ZARAGOZA
Tel. 976 71 4495 • Fax. 976 71 4145
www.aragon.es

Contenido

Entidad Pública Aragonesa de Servicios Telemáticos
Av Pablo Ruiz Picasso, 63 A 3ª J • 50018 ZARAGOZA
Tel. 976 71 4495 • Fax. 976 71 4145
www.aragon.es

1. INTRODUCCIÓN

Vivimos en una época que ha visto la generalización de la sociedad de la información a todos los niveles y la Administración Pública no se ha visto excluida de esta realidad, más bien al contrario, ha tratado no solo de utilizar los medios tecnológicos necesarios para formar parte de la sociedad de la información, sino también de impulsar el uso de dichos medios en la sociedad en general y en las relaciones de los ciudadanos con la Administración en particular

Esta Política desarrolla entre otros aspectos al Comité de Seguridad de las Tecnologías de la Información de Aragonesa de Servicios Telemáticos (Comité de Seguridad TIC de AST en adelante) cuyo objetivo es establecer, gestionar, coordinar y aprobar las actuaciones en materia de seguridad de las tecnologías de la información y las comunicaciones, incluyendo dentro del ámbito de actuación del mismo a todos los sistemas de información del Gobierno de Aragón, de manera que se gestione de forma conjunta la seguridad de dichos sistemas. El motivo es el carácter horizontal de la seguridad y la fuerte interconexión entre todos los sistemas de información que permiten a la Administración Pública prestar su servicio a los ciudadanos.

En el funcionamiento del Comité de Seguridad TIC de AST se promoverá la utilización de medios electrónicos, de conformidad con lo establecido en la disposición adicional primera de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, el cumplimiento de la Ley 39/2017 de Procedimiento Administrativo Común de las Administraciones Públicas, de la Ley 40/2015 del Régimen Jurídico del Sector Público, así como el Reglamento UE2016-679 de Protección de datos.

La Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos consagra el derecho de los ciudadanos a comunicarse electrónicamente con la Administración Pública, dando respuesta también a los compromisos comunitarios y a las iniciativas europeas puestas en marcha a partir del Consejo Europeo de Lisboa. La Ley 11/2007, de 22 de junio, ha sido derogada por la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y su regulación ha sido asumida por esta última ley y por la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

Esta Ley manifiesta la necesidad de una adecuada protección de la información y de los servicios que permita usar los medios electrónicos con confianza y a esta necesidad responde la publicación 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.

El Esquema Nacional de Seguridad tiene como finalidad crear las condiciones de confianza necesarias en el uso de los medios electrónicos, mediante medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos, que permitan a los ciudadanos y a las Administraciones Públicas el ejercicio de derechos y el cumplimiento de deberes a través de estos medios. Actualmente los sistemas de información de las Administraciones Públicas están fuertemente imbricados entre sí, siendo la seguridad una función transversal a todos ellos, por lo que la seguridad tiene un nuevo reto que va más allá del aseguramiento individual de cada sistema. Por ello, entre las obligaciones que impone el mencionado Esquema Nacional se encuentran la de que todos los órganos superiores de las Administraciones públicas deberán disponer formalmente de su política de seguridad que será aprobada por el titular del órgano superior correspondiente, impulsar y verificar la realización de auditorías periódicas de los sistemas de información e informar del estado de la seguridad a los órganos competentes.

Entidad Pública Aragonesa de Servicios Telemáticos
Av Pablo Ruiz Picasso, 63 A 3ª J • 50018 ZARAGOZA
Tel. 976 71 4495 • Fax. 976 71 4145
www.aragon.es

En el citado Real Decreto 3/2010 de 8 de enero, en el anexo II, apartado 3.1.d), Política de seguridad, se establece la existencia de un Comité para la gestión y coordinación de la seguridad.

Entidad Pública Aragonesa de Servicios Telemáticos
Av Pablo Ruiz Picasso, 63 A 3ª J • 50018 ZARAGOZA
Tel. 976 71 4495 • Fax. 976 71 4145
www.aragon.es

2. CAPÍTULO I

Disposiciones generales

2.1. Artículo 1. Objeto

1. La Política tiene por objeto definir y regular la política de seguridad de la información y comunicaciones de Aragonesa de Servicios Telemáticos, en adelante AST, que se ha de aplicar en el tratamiento de los activos de tecnologías de la información y comunicaciones de su titularidad o cuya gestión tenga encomendada, conformando, junto a la normativa que lo desarrolle, el cuerpo normativo de seguridad TIC de AST.

2. Sin perjuicio de las directrices establecidas en el marco normativo de seguridad TIC de la Administración del Gobierno de Aragón, a la que AST pertenece, Aragonesa de Servicios Telemáticos desarrollará y aprobará el documento de política de seguridad TIC, así como las normas y procedimientos que adecuen, en su caso, las directrices comunes de la Administración del Gobierno de Aragón a sus particularidades.

2.2. Artículo 2. Misión u objetivos del Organismo

1. La entidad pública Aragonesa de Servicios Telemáticos tiene como objetivos generales el cumplimiento y ejecución de las directrices estratégicas del Gobierno de Aragón en materia de servicios y sistemas corporativos de información y de telecomunicaciones. Actuando como proveedor principal ante la Administración de la Comunidad Autónoma de Aragón para la cobertura global de las necesidades de ésta en relación con los servicios, sistemas y aplicaciones para la información y las telecomunicaciones.

2. Más concretamente en el ámbito de la seguridad, proponer, implantar y coordinar los medios técnicos que garanticen la seguridad, integridad, calidad y confidencialidad de los sistemas de información y telecomunicaciones de la Administración de la Comunidad Autónoma de Aragón.

2.3. Artículo 3. Marco Normativo

1. A los efectos previstos en esta Política, el marco normativo de referencia es que estipula la legislación vigente en materia de seguridad TIC y en concreto el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad.

2. Así mismo, las definiciones han de ser entendidas en el sentido indicado en el Glosario de términos incluido como Anexo I.

3. Por último, se reconocen como referencias válidas en lo que a la seguridad de los activos TIC de Aragonesa de Servicios Telemáticos se refiere, entre otros, los estándares recogidos en el Anexo II.

Entidad Pública Aragonesa de Servicios Telemáticos
Av Pablo Ruiz Picasso, 63 A 3ª J • 50018 ZARAGOZA
Tel. 976 71 4495 • Fax. 976 71 4145
www.aragon.es

2.4. Artículo 4. Ámbito de aplicación

La Política será de aplicación a Aragonesa de Servicios Telemáticos y a las empresas colaboradoras con las que tiene contratos de colaboración para la gestión y administración de sus sistemas.

2.5. Artículo 5. 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 de Aragonesa de Servicios Telemáticos, en adelante política de seguridad TIC de Aragonesa de Servicios Telemáticos, persigue la consecución de los siguientes objetivos:

a) Garantizar a todo el Gobierno de Aragón que los datos alojados en AST 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 la Administración del Gobierno de Aragón, que cubra en un ciclo continuo de mejora los aspectos técnicos, organizativos y procedimentales.

e) Hacer patente el compromiso de Aragonesa de Servicios Telemáticos 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 Aragonesa de Servicios Telemáticos.

g) Garantizar la continuidad de los servicios ofrecidos por Aragonesa de Servicios Telemáticos a Gobierno de Aragón.

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 controles implantados y aumente la confianza de nuestros clientes.

Entidad Pública Aragonesa de Servicios Telemáticos
Av Pablo Ruiz Picasso, 63 A 3ª J • 50018 ZARAGOZA
Tel. 976 71 4495 • Fax. 976 71 4145
www.aragon.es

3. CAPÍTULO II

Principios de seguridad TIC

3.1. Artículo 6. Principios básicos de la política de seguridad TIC

La política de seguridad TIC de Aragonesa de Servicios Telemáticos se desarrollará, con carácter general, de acuerdo a los siguientes principios:

a) Principio de confidencialidad: los activos TIC deberán ser accesibles únicamente para aquellas personas usuarias, órganos y entidades o procesos expresamente autorizados para ello, con respecto a las obligaciones de secreto y sigilo profesional.

b) Principio de integridad y calidad: se deberá garantizar el mantenimiento de la integridad y calidad de la información, así como de los procesos de tratamiento de la misma, estableciéndose los mecanismos para asegurar que los procesos de creación, tratamiento, almacenamiento y distribución de la información contribuyen a preservar su exactitud y corrección.

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

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

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

f) Principio de gestión del riesgo 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 de Aragonesa de Servicios Telemáticos.

Entidad Pública Aragonesa de Servicios Telemáticos
Av Pablo Ruiz Picasso, 63 A 3ª J • 50018 ZARAGOZA
Tel. 976 71 4495 • Fax. 976 71 4145
www.aragon.es

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.

3.2. Artículo 7. Requisitos Mínimos de Seguridad

Esta política de seguridad, se establece de acuerdo con los principios básicos indicados y se desarrolla aplicando los siguientes requisitos mínimos:

a) Organización e implantación del proceso de seguridad.

b) Análisis y gestión de los riesgos.

c) Gestión de personal.

d) Profesionalidad.

e) Autorización y control de los accesos.

f) Protección de las instalaciones.

g) Adquisición de productos.

h) Seguridad por defecto.

i) Integridad y actualización del sistema.

j) Protección de la información almacenada y en tránsito.

k) Prevención ante otros sistemas de información interconectados.

l) Registro de actividad.

m) Incidentes de seguridad.

n) Continuidad de la actividad.

o) Mejora continua del proceso de seguridad.

Todos estos requisitos mínimos se exigirán en proporción a los riesgos identificados en cada sistema, pudiendo algunos no requerirse en sistemas sin riesgos significativos, y se cumplirán teniendo en cuenta los activos que constituyen el sistema, la categorización del propio sistemas en función de la información gestionada y el servicio prestado, y las decisiones que se adopten para gestionar los riesgos identificados.

Entidad Pública Aragonesa de Servicios Telemáticos
Av Pablo Ruiz Picasso, 63 A 3ª J • 50018 ZARAGOZA
Tel. 976 71 4495 • Fax. 976 71 4145
www.aragon.es

4. CAPÍTULO III

Organización de la seguridad TIC

4.1. Artículo 8. Responsabilidad general

La preservación de la seguridad TIC será considerada objetivo común de todas las personas al servicio de Aragonesa de Servicios Telemáticos, 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, AST se reserva el derecho de aplicar el régimen disciplinario establecido en el Estatuto Básico del Empleado Público aprobado por Real Decreto Legislativo 5/2015, de 30 de octubre y en las normas que las Leyes de Función Pública dicten en desarrollo del mismo.

Las atribuciones de cada responsable, entre ellos el Responsable de Información, Responsable de Servicio, Responsable de Sistemas y Responsable de Seguridad, así como los mecanismos de coordinación y resolución de conflictos se explicitan en las Normativa que AST tiene de Roles, Responsabilidades de Seguridad en AST que permiten una gestión adecuada y a los niveles requeridos de la seguridad.

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

4.2. Artículo 9. Comité de Seguridad TIC de AST

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

2. El Comité estará formado por la Gerencia y los Directores en representación de sus Áreas y el Responsable de Seguridad TIC.

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.

Entidad Pública Aragonesa de Servicios Telemáticos
Av Pablo Ruiz Picasso, 63 A 3ª J • 50018 ZARAGOZA
Tel. 976 71 4495 • Fax. 976 71 4145
www.aragon.es

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 de Aragonesa de Servicios Telemáticos.

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

4.3. Artículo 10. Responsable de seguridad TIC

1. El nombramiento del Responsable de Seguridad será potestad del Comité de Seguridad TIC de AST.

2. La persona Responsable de Seguridad TIC tendrá las siguientes funciones:

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) Desarrollo y seguimiento de programas de formación y concienciación.

e) Reporte al Comité de Seguridad TIC 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 UE2016-679 que regula la Protección de Datos de Carácter Personal, aprobado el 25 de mayo de 2016 y que entra en vigor el 25 de mayo de 2017.

4.4. Artículo 11. Oficina de Seguridad TIC

1. La Oficina de Seguridad TIC estará compuesto por los Responsables de Área de AST, 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 TIC de AST que tendrá funciones sobre la elaboración de propuestas para ser presentadas y debatidas en el Comité de Seguridad TIC de AST.

Entidad Pública Aragonesa de Servicios Telemáticos
Av Pablo Ruiz Picasso, 63 A 3ª J • 50018 ZARAGOZA
Tel. 976 71 4495 • Fax. 976 71 4145
www.aragon.es

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 de AST.

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 de AST.

4. La Oficina de Seguridad TIC se reunirá al menos una vez por trimestre, y se regirá por esta Política.

El funcionamiento detallado de la Organización de la Seguridad en AST está pormenorizado en la Normativa de Roles y Responsabilidades de la Seguridad IT de AST y la Normativa de Gestión de la Seguridad.

Mayte Ortín Puértolas

Directora-Gerente de Aragonesa de Servicios Telemáticos

(documento firmado electrónicamente)

Entidad Pública Aragonesa de Servicios Telemáticos
Av Pablo Ruiz Picasso, 63 A 3ª J • 50018 ZARAGOZA
Tel. 976 71 4495 • Fax. 976 71 4145
www.aragon.es

5. 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.

Entidad Pública Aragonesa de Servicios Telemáticos
Av Pablo Ruiz Picasso, 63 A 3ª J • 50018 ZARAGOZA
Tel. 976 71 4495 • Fax. 976 71 4145
www.aragon.es

6. ANEXO II

Estándares

a) UNE-ISO/IEC 27001, Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI).

b) UNE-ISO/IEC 27002, Código de buenas prácticas para la Gestión de la Seguridad de la Información.

c) ISO 22301-2012. Gestión de la Continuidad del Negocio.

Entidad Pública Aragonesa de Servicios Telemáticos
Av Pablo Ruiz Picasso, 63 A 3ª J • 50018 ZARAGOZA
Tel. 976 71 4495 • Fax. 976 71 4145
www.aragon.es