ast. Aragón, Servicios y Tecnología

Política de Seguridad Integral de AST

Documento del Sistema Integrado de Gestión de la Cali dad y Seguridad de la Información

Versión pública para publicación web.

Ficha de control documental

Información del documento	
Versión	5.1 - Pública
Clasificación	Público – **TLP:CLEAR**
Autor/es	Centro de Excelencia de Ciberseguridad

Registro de cambios			
Versión	**Fecha**	**Autor**	**Descripción**
5.0	29/06/2025	Ignacio Pérez [AST.ciber]	Cambio estructura AST. Creación del Centro de Ciberseguridad de Aragón y absorción del AST.CERT. asimilación del Comité de Seguridad con el Comité de Dirección. Eliminación de la Comisión Técnica de Seguridad. Cambio en la asignación del Responsable de la Información, del Servicio, así como del Responsable de Seguridad.
5.1	15/06/2026	Centro Excelencia Ciberseguridad	Actualización del documento
5.1 - Pública	27/08/2026	Centro de Excelencia de Ciberseguridad	Adaptación para publicación web

Control de revisiones			
Fecha	**Revisado por**	**Área**	**Próxima revisión**
(ver firma)	Comité de Seguridad [AST]	Todo el documento	23/12/2030

Distribución		
Nombre	**Área**	**Entidad**
*	Todo el documento	AST
*	Todo el documento	Departamentos y organismos públicos de pendientes del Gobierno de Aragón. Así como otras entidades receptoras directas de los servicios prestados por AST
*	Todo el documento	Contratas de AST
*	Todo el documento	Auditores ENS/ISO de AST
*	Todo el documento	Contratas de otras entidades bajo autorización expresa de AST
*	Todo el documento	Red Nacional de SOC y Centro Criptológico Nacional
*	Todo el documento	Oficina de Coordinación Cibernética
*	Todo el documento	Centro Nacional de Protección de Infraestructuras Críticas
*	Todo el documento	Agencia Española de Protección de Datos

Nota sobre la versión pública

El presente documento constituye una versión pública y resumida de la **Política de Seguridad Integral de AST**, elaborada con fines de difusión y publicación externa. Esta versión recoge los principios, compromisos y directrices generales en materia de seguridad de la información, omitiendo aquellos contenidos de carácter interno cuya divulgación no resulta necesaria o pudiera afectar a la seguridad de la organización.

El contenido completo de la Política se encuentra recogido en el documento corporativo **POL_Política de Seguridad Integral**, disponible a través de los canales internos habilitados al efecto.

Asimismo, la organización detallada, las asignaciones específicas de responsabilidades, los procedimientos internos, las capacidades técnicas y el resto de información de acceso restringido se regulan en la documentación interna aplicable

Contenido

Capítulo I. Introducción

Objetivo y alcance de esta Política

La Dirección de Aragonesa de Servicios Telemáticos, en adelante AST, considera que la información, los servicios digitales, los sistemas que los soportan y las personas que intervienen en su prestación constituyen activos esenciales para el cumplimiento de sus fines. En consecuencia, asume la seguridad integral como una responsabilidad corporativa y como un elemento necesario para prestar servicios públicos confiables, resilientes y de calidad.

La presente Política establece el marco general para proteger la información y los servicios frente a amenazas que puedan afectar a su confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad. La seguridad se entiende como un proceso continuo, basado en la gestión del riesgo, la prevención, la detección, la respuesta, la recuperación y la mejora permanente.

La Política forma parte del Sistema de Gestión de AST y sirve de referencia para el desarrollo de normas, procedimientos e instrucciones internas. Su contenido público expresa los compromisos, principios y criterios generales de actuación, sin revelar información sobre la arquitectura tecnológica, las capacidades operativas, las configuraciones, la composición detallada de los órganos internos, los planes de respuesta o continuidad ni otras materias cuya difusión pudiera incrementar la exposición al riesgo.

La Dirección manifiesta su apoyo a la implantación y mejora de las medidas de seguridad, a la gestión coordinada de incidentes, a la continuidad de los servicios, a la concienciación y formación del personal y a la realización de revisiones y auditorías que permitan verificar el cumplimiento y la eficacia de los controles.

Revisión y evaluación

La presente política será revisada de forma periódica, no pasando más de cinco años entre una versión y otra, por el Responsable de Seguridad. La modificación de la siguiente política requerirá la aprobación del comité de seguridad.

Capítulo II. Disposiciones generales

Artículo 1. Objeto

La presente Política tiene por objeto dirigir y dar soporte a la gestión de la seguridad integral de AST, definiendo los principios, objetivos y responsabilidades generales que deben regir la protección de la información, los servicios, los sistemas, las instalaciones y los demás activos vinculados a la actividad de la entidad.

Asimismo, establece el marco de referencia para el cuerpo normativo de seguridad y para la adopción de medidas técnicas, organizativas, físicas y procedimentales adecuadas y proporcionadas a los riesgos.

Artículo 2. Misión u objetivos del Organismo

AST presta servicios y soluciones en el ámbito de las tecnologías de la información, las telecomunicaciones y los servicios digitales para la Administración de la Comunidad Autónoma de Aragón y sus organismos dependientes, contribuyendo a la mejora de los servicios públicos y a la transformación digital del territorio.

En el desarrollo de esta misión, AST se compromete a preservar la confianza de las entidades destinatarias y de la ciudadanía, integrar la seguridad desde el diseño y durante todo el ciclo de vida de los servicios, promover la homogeneidad y la calidad de las soluciones y asegurar que las decisiones se adopten conforme a criterios de legalidad, proporcionalidad y gestión del riesgo.

Artículo 3. Marco legal y regulatorio

Esta Política se aplicará de acuerdo con la legislación vigente y, en particular, con el Esquema Nacional de Seguridad, la normativa de protección de datos personales, la normativa sobre seguridad de las redes y sistemas de información, administración electrónica, servicios de confianza, infraestructuras críticas, seguridad física y demás disposiciones que resulten aplicables.

Como marcos de referencia para la gestión se tendrán en cuenta, entre otros, las normas UNE-EN ISO 9001, UNE-EN ISO/IEC 27001, ISO/IEC 27002, ISO 22301, ISO 31000 e ISO/IEC 27005, así como las guías y recomendaciones emitidas por organismos nacionales, europeos e internacionales competentes en materia de ciberseguridad y gestión de riesgos

Artículo 4. Ámbito de aplicación.

La Política se aplica a las actividades, procesos, servicios, sistemas de información, infraestructuras, instalaciones y activos gestionados por AST, así como al personal propio y externo que participe en su diseño, prestación, operación, mantenimiento, supervisión o soporte.

También será exigible, en los términos previstos contractualmente, a proveedores, colaboradores y terceras partes que accedan a información, sistemas o recursos bajo responsabilidad de AST. Cuando intervengan otras entidades, las obligaciones y mecanismos de coordinación se concretarán mediante los instrumentos jurídicos, contractuales y operativos correspondientes.

Artículo 5. Objetivos de la política de seguridad de las tecnologías de la información y las comunicaciones.

Esta Política persigue los siguientes objetivos:

- Proteger la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información y de los servicios.
- Gestionar los riesgos de forma continua y proporcionar medidas adecuadas a la naturaleza de la información, la criticidad de los servicios y la categoría de los sistemas.
- Prevenir, detectar, responder y recuperarse frente a incidentes, minimizando sus efectos y preservando las evidencias necesarias.
- Garantizar la continuidad y resiliencia de los servicios mediante planes, procedimientos, pruebas y mecanismos de recuperación proporcionados.
- Cumplir la legislación, los requisitos regulatorios, los compromisos contractuales y la normativa interna aplicable.
- Promover una cultura de seguridad basada en la formación, la concienciación, la responsabilidad y el uso adecuado de los recursos.
- Medir la eficacia de los controles y mantener un ciclo de mejora continua apoyado en revisiones, auditorías e indicadores.

Capítulo III. Doctrina de Seguridad

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 con los siguientes principios:

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.

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.

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.

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.

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.

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.

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.

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.

Principio de Prevención, detección, respuesta y conservación.: La seguridad del sistema debe contemplar las acciones relativas a los aspectos de prevención, detección y respuesta, al objeto de minimizar sus vulnerabilidades y lograr que las amenazas sobre el mismo no se materialicen

o que, en el caso de hacerlo, no afecten gravemente a la información que maneja o los servicios que presta.

Principio de vigilancia, mejora continua y 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. Se buscarán detección de actividades o comportamientos anómalos y su oportuna respuesta e impulsar la evaluación permanente del estado de la seguridad de los activos, para detectar vulnerabilidades e identificar deficiencia de configuración.

Principio de seguridad 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.

Principio de defensa en profundidad o líneas de defensa: El sistema de información ha de disponer de una estrategia de protección constituida por múltiples capas de seguridad, dispuesta de forma que, cuando una de las capas sea comprometida, permita tanto desarrollar una reacción adecuada frente a los incidentes que no han podido evitarse reduciendo la probabilidad de que el sistema sea comprometido en su conjunto, como minimizar el impacto final sobre el mismo.

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.

Principio de seguridad global: Ante cualquier decisión, diseño o configuración, se ha de adoptar la máxima de la seguridad por defecto. Cuando un sistema, por cuestiones de negocio, rebaje el nivel de seguridad, este ha de ser aislado en la medida de lo posible. Evitando en todo momento que comprometa la seguridad global o de otros entornos asociados.

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. 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 de acuerdo en cuenta los activos que constituyen el sistema, la categorización de los propios sistemas en función de la información gestionada y el servicio prestado y las decisiones que se adopten para gestionar los riesgos identificados.

Las directrices para cumplir estos requisitos mínimos se establecen, tal y como marca la Política del Sistema de Gestión y el anexo mapa de procesos en diferentes documentos del Sistema Integrado de Gestión[4] Se puede ver una relación orientativa de los mismos en el 0 .

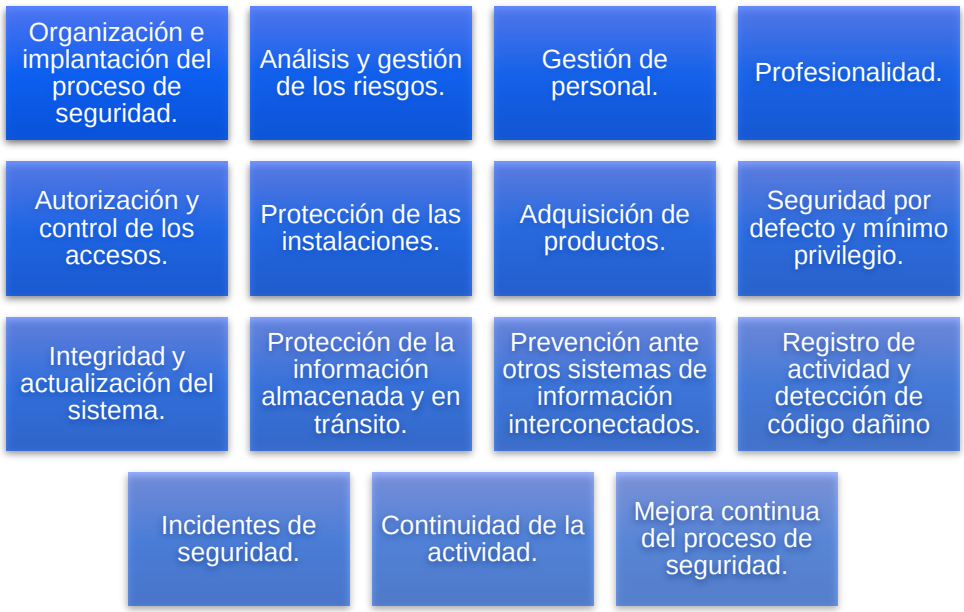

Ilustración 1. Requisitos mínimos de seguridad

Artículo 8. Carácter Integral de la Seguridad

La seguridad física y la seguridad de la información son áreas que dentro de AST se abordan de forma interrelacionada y con una perspectiva holística de la seguridad. Redundando en una visión global de la seguridad, posibilitando el diseño de una estrategia corporativa única, y optimizando el conocimiento, los recursos y los equipos.

AST cuenta con unos activos físicos necesarios para cumplir con su misión y objetivos. Estos activos físicos están sujetos a las mismas dimensiones de seguridad que los activos de información intangibles. Dado de este carácter integral de la seguridad aplicada a ambos tipos de activos se aplicará, en la medida de lo posible y con los matices necesarios, los mismos procesos para alcanzar dicha seguridad integral. En este sentido, una respuesta integral a las diferentes amenazas existentes requiere la aplicación coordinada de medidas de seguridad física y ciberseguridad.

Artículo 9. Estrategias de seguridad

Para mantener los riesgos dentro de los niveles aceptados y recuperar la operación tras un incidente, AST aplicará las siguientes líneas de actuación:

- Alineación de todo el personal y de las terceras partes con las políticas, normas y directrices de seguridad.
- Reducción de la superficie y del tiempo de exposición mediante accesos limitados, necesidad de conocer, mínimo privilegio y revisión periódica de autorizaciones.
- Preparación frente a contingencias, con planes documentados, responsabilidades asignadas, pruebas periódicas y mecanismos de recuperación.
- Respuesta coordinada y ágil ante incidentes, priorizando la contención, la continuidad, la protección de las personas y la reducción del impacto.
- Automatización y estandarización cuando sean seguras, eficaces y estén suficientemente probadas.
- Defensa en profundidad y segmentación para limitar la propagación y evitar fallos únicos.
- Supervisión continua, gestión de vulnerabilidades, actualización y corrección de configuraciones deficientes.
- Gestión responsable de proveedores y dependencias tecnológicas, favoreciendo la interoperabilidad, la reversibilidad y la continuidad del servicio.

Artículo 10. Marcos de referencia

AST adopta el Esquema Nacional de Seguridad como marco legal básico y mantiene un sistema de gestión alineado con normas internacionales reconocidas. Los procedimientos internos podrán incorporar metodologías y buenas prácticas del Centro Criptológico Nacional, ENISA, NIST, CIS, MITRE, ITIL y otros marcos aplicables, cuando aporten valor y sean compatibles con las obligaciones de la entidad

Capítulo IV. Organización de la seguridad y funciones

Artículo 11. Responsabilidades Esenciales

La responsabilidad del éxito de una Organización recae, en última instancia, en su Dirección. La Dirección es responsable de organizar las funciones y responsabilidades, la política de seguridad del Organismo, y de facilitar los recursos adecuados para alcanzar los objetivos propuestos.

La seguridad de la información es responsabilidad de todas las personas que acceden a la información o utilizan los sistemas de la organización.

Artículo 12. Modelo de gobierno de la seguridad

AST dispondrá de órganos de gobierno, coordinación y operación adecuados a su actividad. El modelo diferenciará los niveles estratégicos, de supervisión y operativo, y establecerá mecanismos para la toma de decisiones, el seguimiento, la rendición de cuentas y la resolución de conflictos.

La composición detallada, las reglas de funcionamiento, los canales de escalado y los procedimientos de actuación se mantienen en la documentación interna y se revisan conforme a las necesidades de la entidad. Esta reserva evita exponer información organizativa u operativa que pudiera ser utilizada para eludir controles o dirigir acciones contra personas, servicios o activos concretos.

Artículo 13. Roles y segregación de funciones

Se identificarán y asignarán los roles previstos en el Esquema Nacional de Seguridad, incluyendo las responsabilidades sobre la información, los servicios, la seguridad y los sistemas. Las atribuciones se documentarán, comunicarán y revisarán, preservando la independencia de la función de seguridad respecto de la operación ordinaria de los sistemas.

Los responsables determinarán los requisitos de protección, impulsarán su implantación, supervisarán su eficacia y comunicarán los riesgos y desviaciones a los órganos competentes. Las funciones podrán delegarse cuando resulte necesario, sin que la delegación extinga la responsabilidad de quien la realiza

Artículo 14. Protección de datos y terceras partes

El tratamiento de datos personales se realizará conforme al Reglamento General de Protección de Datos, la Ley Orgánica 3/2018 y demás normativa aplicable. La persona Delegada de Protección de Datos ejercerá sus funciones con independencia, asesorará y supervisará el cumplimiento y actuará como punto de contacto con las autoridades de control.

Los proveedores y entidades colaboradoras deberán aplicar las medidas de seguridad establecidas y designar interlocutores adecuados cuando la naturaleza del servicio lo requiera. Los contratos incorporarán obligaciones sobre confidencialidad, control de accesos, gestión de incidentes, continuidad, auditoría, devolución o destrucción de información y finalización ordenada del servicio

Artículo 15. Sistema de gestión y supervisión

La seguridad se gestionará dentro del Sistema Integrado de Gestión de AST mediante procesos documentados de planificación, operación, evaluación y mejora. Se realizarán análisis de riesgos, seguimiento de objetivos, control de cambios, gestión de incidentes, auditorías y revisiones periódicas, manteniendo las evidencias necesarias para acreditar el cumplimiento.

Las desviaciones y riesgos residuales serán tratados y, cuando proceda, aceptados por los órganos con autoridad suficiente. Las medidas compensatorias deberán estar justificadas, documentadas, aprobadas y sometidas a seguimiento

Artículo 16. Desarrollo normativo

Esta Política se desarrollará mediante políticas específicas, normas, procedimientos, instrucciones técnicas, planes y registros de obligado cumplimiento. Dicha documentación concretará las medidas aplicables, los responsables, los controles, las evidencias y los mecanismos de revisión. Su acceso se limitará conforme a su clasificación y a la necesidad de conocer.

La versión pública de esta Política prevalece únicamente como declaración institucional de principios y compromisos. La aplicación operativa se regirá por la versión completa aprobada y por la normativa interna vigente.

Capítulo V. Anexos

Anexo I. Glosario

CCN: Centro Criptológico Nacional

CERT: Computer Emergency Response Team

CSIRT: Computer Security Incident Response Team

Empleado: personal propio del Gobierno de Aragón o de cualquier entidad u organismo público asociado al mismo.

ENS: Esquema Nacional de Seguridad

Proveedor, o **contratista**: Se refiere a las entidades, o al personal perteneciente a empresas externas, con relación contractual con AST, o con algún otro organismo público, y que requiera utilizar recursos gestionados por AST para el desarrollo de su contrato. Existen normas que les aplican específicamente

Usuario: Cualquier empleado público perteneciente o ajeno a AST, así como personal de organizaciones privadas externas, entidades colaboradoras o cualquier otro con algún tipo de vinculación con AST y que utilice o posea acceso a los Sistemas de Información de AST.