POLÍTICA DE SEGURIDAD

1.- INTRODUCCIÓN

Aernnova está especializada en el diseño, fabricación y mantenimiento de aeroestructuras de tecnología avanzada, así como de los componentes, sistemas y equipamientos relacionados con las mismas, contribuyendo con su Misión a conectar a las personas y al desarrollo económico y social.

El Consejo de Administración de Aernnova Aerospace Corporation ha aprobado esta Política de Seguridad para su aplicación en las actividades mencionadas.

.2- OBJETO

Esta Política de Seguridad establece los principios de gestión y el compromiso de la dirección para la protección del personal, de la información y los recursos de tecnología asociados a la misma, y de los activos de Aernnova, así como para preservar la operación segura de los procesos y de los productos entregados y en servicio.

Las medidas de seguridad en Aernnova están destinadas a:

• Proteger al personal, actividades y activos de valor (información, patrimonio tecnológico, instalaciones y reputación) contra cualquier acto hostil o vulnerabilidad que pudiera comprometer su seguridad o la seguridad aérea.

• Preservar la privacidad del personal y la confidencialidad de nuestros clientes.

• Prevenir, detectar y responder a cualquier acto hostil, accidental o intencionado, en contra del personal, las actividades y activos de valor o de la seguridad aérea.

• Satisfacer los requisitos aplicables en materia de seguridad y de seguridad de la información: regulatorios, contractuales u otros propios que la organización suscriba, considerando las normas y mejores prácticas de la industria, así como las expectativas sociales.

• Proporcionar un marco de referencia para establecer los objetivos y medir el rendimiento de la seguridad de la información y proporcionar la mejora continua del sistema alcanzando mayores niveles de seguridad.

Ed. 2 Rev. 2	17/07/2025	General Update
Ed. 2 Rev. 1	22/05/2025	General Update
Ed. 2 Rev. 0	12/06/2023	General Update
Ed. 1 Rev. 0	02/07/2018	First Edition

3- PRINCIPIOS BÁSICOS

• Los niveles de seguridad requeridos tendrán en cuenta el análisis de riesgos realizado por Aernnova, el cual se realizará de forma periódica y conforme a los procedimientos aplicables.

• Todo el personal de Aernnova deberá cumplir con esta Política y la documentación y normativa interna relacionada.

• Los requerimientos derivados de esta Política se extenderán a terceras partes asociadas.

• Se fomentará una cultura de seguridad con transparencia y comunicación abierta, alentando al personal a notificar cualquier vulnerabilidad, evento anómalo o sospechoso, o incidente de seguridad en una atmósfera de confianza y responsabilidad. Se respetará en todo momento el principio de Cultura Justa, según la cual las personas no son castigadas por acciones, omisiones o decisiones tomadas conforme a su experiencia y entrenamiento, pero no se toleran negligencias graves, la ocultación, violaciones intencionales o actos destructivos o ilícitos.

• Los activos corporativos e información confidencial o restringida serán protegidos contra todas las formas de acceso, uso, copia, divulgación, modificación y destrucción asegurando su confidencialidad, integridad y disponibilidad, conforme a los requisitos legales, contractuales y regulatorios aplicables.

Responsabilidades

La consecución de un nivel adecuado de seguridad requiere la participación de toda la organización de Aernnova:

1. Responsabilidades del personal

Se fomentará la cultura de seguridad en la Organización mediante formación y comunicaciones de promoción de la seguridad.

La participación del personal es clave observando las prescripciones de seguridad, los reglamentos y los procedimientos internos.

Cada profesional debe tener el debido cuidado de su propio espacio de trabajo, de las herramientas, equipos, recursos tecnológicos y de información y datos (en adelante, activos) conforme a lo dispuesto por Aernnova, nuestros Clientes y Proveedores, para la realización de sus deberes profesionales.

El acceso y uso a estos activos cesará cuando dejen de ser necesarios.

2. Responsabilidades del Comité de Seguridad

El Comité de Seguridad tendrá la responsabilidad de garantizar la aplicación y el mantenimiento del Sistema de Gestión de Seguridad de Aernnova. Esto incluye el supervisar la correcta aplicación de la normativa de seguridad, y la prestación de asistencia de consultoría en:

• política, manuales, directivas, normas, procedimientos y directrices de interpretación y cumplimiento

• la ejecución técnica y de procedimiento,

• comunicaciones,

• la realización de auditorías y revisiones para el cumplimiento de políticas y evaluaciones de riesgos.

• la evaluación y mejora continua de esta política y de la eficacia del sistema de gestión de la seguridad. Se evaluarán anualmente o con mayor frecuencia si es necesario, para adaptarse a cambios en los riesgos, regulaciones o el entorno organizacional.

El Comité de Seguridad velará por que las políticas o procedimientos, globales o locales sean coherentes con los requisitos de esta política.

3. Responsabilidades de terceros

El personal de contratas y subcontratas serán responsables de observar estas reglas cuando accedan a instalaciones, activos e información de Aernnova.

A tal efecto, las directivas de seguridad de Aernnova se comunicarán a terceros, y si es necesario, se agregará como anexo a la documentación contractual correspondiente.

Principios de seguridad

Los siguientes principios se aplicarán en las Directivas específicas, procedimientos, estándares y directrices

1. Controles de accesos

La seguridad física se gestionará mediante sistemas de control de accesos, que garanticen una entrada segura y regulada a las instalaciones. El acceso a los edificios se gestionará mediante una combinación de controles tecnológicos y de procedimiento, que garanticen que sólo entren el personal y visitantes autorizados, al tiempo que se mantiene un entorno seguro que protege a nuestra plantilla, activos e información.

La gestión de visitantes y el acceso del personal se regirán por directivas y protocolos claros, que garanticen que los accesos se conceden en función de los requisitos de

la función y la finalidad del visitante, y estarán sujetos a revisiones y auditorías periódicas para garantizar la seguridad permanente y el cumplimiento de las normas reglamentarias.

2. Seguridad física y operativa

El acceso a todos los activos protegidos de la empresa se registrará y supervisará de conformidad con las normas locales, observando los procedimientos definidos a tal efecto.

Se aplicarán directrices y formación rigurosas para el personal de seguridad, garantizando el uso mínimo y proporcionado de la fuerza, respetando la libertad de movimiento y manteniendo la transparencia, la responsabilidad y el respeto de los derechos individuales en todas las operaciones de seguridad.

3. Viajes de Negocios y misión en el extranjero

El cuidado apropiado, la asistencia y el asesoramiento deberán estar asegurados para el personal que viaja y/o trabaja en el extranjero ya que pueden estar expuestos a riesgos de seguridad en algunos países o lugares.

4. Seguridad de la información

AERNNOVA se compromete a garantizar la seguridad de nuestros sistemas informáticos al tiempo que da prioridad a la privacidad de cada persona, la integridad de los datos y la disponibilidad del sistema, adhiriéndose a las normas éticas y legales más estrictas en todas las interacciones y controles digitales.

Aspiramos a mantener la transparencia en nuestras prácticas digitales y aplicarlas de forma que mantengan una funcionalidad y accesibilidad óptimas, con el objetivo de salvaguardar la integridad del sistema y de los datos sin ponerlos en peligro.

5. Control de la información

Se desarrolla y mantiene un marco sólido de seguridad de la información que garantice que las personas autorizadas tengan un acceso preciso a la información que necesitan, al tiempo que se evitan diligentemente los accesos no autorizados.

Mediante la aplicación de controles sólidos, protegeremos la integridad y disponibilidad de la información y alinearemos nuestras prácticas con un enfoque global que dé prioridad a la confidencialidad, la resistencia a las ciber amenazas y el cumplimiento de la normativa.

Aernnova implementa controles de seguridad para garantizar la confidencialidad de la información, asegurando que solo las personas autorizadas accedan a datos sensibles. La información será protegida durante todo su ciclo de vida y se garantizará el cumplimiento de estas medidas por parte de empleados, proveedores y terceros mediante acuerdos de confidencialidad y medidas de seguridad adecuadas.

Ed. 2 Rev. 2	17/07/2025	General Update
Ed. 2 Rev. 1	22/05/2025	General Update
Ed. 2 Rev. 0	12/06/2023	General Update
Ed. 1 Rev. 0	02/07/2018	First Edition

6. Recuperación ante Desastres / Continuidad del Negocio

Los eventos que pueden causar interrupciones en los procesos de negocio deben ser identificados, junto con la probabilidad y el impacto de estas interrupciones y de sus consecuencias para la seguridad de la información.

Los planes y procedimientos de continuidad de negocio se mantendrán, probados y actualizados para garantizar la continua disponibilidad de los procesos de negocio.

7. Gestión de Incidentes

Se implantará un proceso estructurado de gestión de incidentes para identificar, responder y mitigar los incidentes de seguridad de forma oportuna y eficaz, así como para la notificación interna y externa de los mismos.

El proceso deberá incluir canales de información claros, funciones y responsabilidades definidas y un enfoque sistemático del análisis, la documentación y la comunicación de incidentes para garantizar que los incidentes se gestionan con eficacia y que las lecciones aprendidas se incorporan a las prácticas de seguridad en curso.

4-. SISTEMAS DE CONTROL

Todos los directivos de Aernnova son responsables (en su ámbito de actuación) de velar por la implementación y revisión periódica de esta política y del Sistema de Gestión de la Seguridad definido en el Manual (MDG-00-401) y de asignar los recursos necesarios para su cumplimiento, incluyendo personal, tecnología e infraestructura, y el presupuesto necesario para la implementación y operación efectiva del del Sistema de Gestión de Seguridad de la Información (SGSI).

Se determinarán y documentarán las competencias necesarias para el personal involucrado en actividades relacionadas con la seguridad de la información. Estas competencias estarán disponibles y se evaluarán periódicamente para asegurar que el personal cuente con los conocimientos adecuados para cumplir con sus responsabilidades.

El sistema de Control incluye, pero no se limita a:

• La implantación del sistema de seguridad operacional descrito en MDG-00-401 y en los procedimientos asociados, que asegure la protección de las personas y activos de las diferentes entidades que componen Aernnova y la confidencialidad, integridad y disponibilidad de la información en la red global de Aernnova.

• Asegurarse, mediante un sistema de información de eventos de seguridad, de que toda la información relativa a la seguridad esté notificada y gestionada adecuadamente.

Ed. 2 Rev. 2	17/07/2025	General Update
Ed. 2 Rev. 1	22/05/2025	General Update
Ed. 2 Rev. 0	12/06/2023	General Update
Ed. 1 Rev. 0	02/07/2018	First Edition

• Se establecerán indicadores adecuados para la evaluación de la eficacia del sistema y objetivos periódicos de mejora continua.

• El sistema de control incluye la realización de auditorías internas para evaluar anualmente el cumplimiento de los requisitos regulatorios, contractuales u otros que la organización suscriba, así como la implantación efectiva y mantenimiento del SGSI.

La dirección supervisa regularmente el desempeño del SGSI como se establece en la revisión del Sistema, asegurando que esté alineado con los objetivos estratégicos de Aernnova y fomentando una cultura organizacional que valore la seguridad de la información.

5- COMUNICACIÓN E INVOLUCRACIÓN DE LOS GRUPOS DE INTERÉS

La Política de Seguridad se dirige a todas las Partes Interesadas: Clientes, Autoridades, Accionistas, Personal de Aernnova, Proveedores y Consumidores y Sociedad en su conjunto. Aernnova reconoce la importancia de identificar y comprender a las partes interesadas clave, tanto internas como externas, que afectan y se ven afectadas por sus actividades, así como las leyes, regulaciones y contratos aplicables. Además, Aernnova asegura que cumple con las regulaciones aplicables relacionadas con la seguridad de la información, tanto a nivel local como global, y mantiene un proceso continuo de revisión y ajuste de sus prácticas y procedimientos para adaptarse a cualquier cambio legislativo o normativo. Esto asegura la protección continua de la confidencialidad, integridad y disponibilidad de la información.

Aernnova identifica y evalúa de manera continua las expectativas, requisitos específicos de seguridad de la información, y las obligaciones legales y contractuales de las partes interesadas.

Se ha comunicado y se entiende dentro del alcance de la organización, y está disponible a través de los canales de comunicación e información que la compañía pone a disposición de las partes interesadas. Está disponible públicamente en la web de AERNNOVA.