



POLÍTICA DE SEGURIDAD

1.- INTRODUCCIÓN

Aernnova está especializada en el diseño, fabricación y mantenimiento de aerestructuras 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.

.2- OBJETO

El propósito de esta política es establecer un marco general de referencia para la protección del personal, de la información y los recursos de tecnología asociados a la misma y de los activos de Aernnova.

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 que pudiera comprometer su seguridad.
- 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.

3- PRINCIPIOS BÁSICOS

- Los niveles de seguridad requeridos se basarán en el análisis de riesgos realizado por Aernnova.
- Todo el personal de Aernnova deberá cumplir con esta Política y la documentación y normativa interna relacionada.
- Los requerimientos derivados de esta Política obligarán por contrato a terceras partes asociadas.
- Los activos corporativos e información confidencial o restringida serán protegidos contra todas las formas de acceso, uso, copia, divulgación, modificación y destrucción.

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

Responsabilidades

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

1. Responsabilidades del personal

El personal de Aernnova deberán observar 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.

Todo el personal deberá garantizar que estos activos son debidamente entregados cuando ya no sean 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.

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 contratistas y subcontratistas 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

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

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. Sistemas de Tecnología de Información y Comunicación (TIC)

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 debe desarrollar y mantener 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

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

global que dé prioridad a la confidencialidad, la resistencia a las ciber amenazas y el cumplimiento de la normativa.

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.

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

La Dirección de Aernnova es responsable (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)

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

- La implantación de un sistema de seguridad operacional que asegure la protección de las personas y activos de las diferentes entidades que componen Aernnova.
- El establecimiento de políticas y procedimientos de seguridad de los sistemas de información cuya finalidad es proteger 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

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. 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.

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