POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y DE LA CONTINUIDAD DEL NEGOCIO (SGSICN):

Objetivo

El objetivo global de Seguridad de la Información y Continuidad del negocio de **ARIETE SEGURIDAD SA** (en adelante **ARIETE SEGURIDAD**) es asegurar la continuidad del negocio, la protección de la información y la calidad los servicios ofrecidos a nuestros clientes minimizando al mínimo los riesgos de seguridad y empresariales, mediante la prevención de incidentes de seguridad, así como la reducción de su impacto potencial cuando sea inevitable.

Para lograr este objetivo, **ARIETE SEGURIDAD** ha desarrollado una metodología de gestión del riesgo que permite analizar regularmente el grado de exposición de nuestros activos importantes frente a aquellas amenazas que puedan aprovechar ciertas vulnerabilidades e introduzcan impactos adversos a las actividades de nuestro personal o a los procesos importantes de **ARIETE SEGURIDAD**.

1. Alcance

Esta política apoya la política general de protección de datos personales, seguridad de la información y continuidad del negocio de **ARIETE SEGURIDAD** y del resto de las políticas y procedimientos del SGSICN que dan soporte a los servicios relacionados con la Vigilancia y gestión en centros de control CTV, Vigilancia presencial, Seguridad de control de accesos, apertura y cierres, Seguridad aeroportuaria y Control y registro de visitas.

2. Responsabilidades

La Dirección es responsable de asegurar y de dotar los recursos necesarios para que la seguridad de la información se gestiona adecuadamente en toda la organización.

El responsable de seguridad es encargado de revisar y aprobar las diferentes estrategias y procesos de seguridad de la información, velando por su calidad y efectividad, así como, proporcionar apoyo especializado al personal de la organización.

Cada miembro del personal tiene la responsabilidad de mantener la seguridad de información dentro de las actividades relacionadas con su trabajo.

3. Política del Sistema

- Garantizar y asegurar la seguridad de la información y de los datos personales siendo requisito estratégico y de importancia vital para prestar nuestros servicios, asegurando y garantizando la confidencialidad, integridad, disponibilidad y privacidad de la información propia y de nuestros clientes.
- La Dirección, para alcanzar los objetivos, proporcionará los recursos adecuados para el mantenimiento y mejora del SGSICN, participa activamente en el establecimiento, seguimiento y revisión de objetivos estratégicos.
- **ARIETE SEGURIDAD** se responsabilizará de la gestión de los riesgos clave para la seguridad de la información y la continuidad operativa de los procesos considerados críticos para la organización.
- Definir, desarrollar e implantar los controles técnicos y organizativos que resulten necesarios para garantizar la Confidencialidad, Integridad y Disponibilidad de la información gestionada en **ARIETE SEGURIDAD**.
- Garantizar el cumplimiento de la legislación vigente en materia de protección de datos de carácter personal, propiedad intelectual y seguridad privada, así como de todos aquellos requerimientos legales, reglamentarios y contractuales que resulten aplicables.
- Definir los requisitos de formación en seguridad y proporcionar la formación necesaria en dicha materia a las partes interesadas, mediante el establecimiento de planes de formación.
- Crear una “cultura de seguridad y de privacidad” tanto internamente, en relación con todo el personal, como externamente, en relación con los clientes y proveedores.
- Elaborar un Plan de Continuidad de la información que permita recuperarse ante un desastre, en el menor tiempo posible.
- Minimizar los riesgos de seguridad de la información, asegurando planes de respuesta eficaces ante incidentes.

- Considerar el Sistema de Gestión de Seguridad de la Información y la Continuidad del Negocio como un proceso de mejora continua, ejecutando revisiones periódicas con el objetivo de alcanzar cada vez mayores niveles de madurez de seguridad de la información.
- El cumplimiento de esta política, así como de la política de seguridad de la información y de cualquier procedimiento o documentación incluida dentro del repositorio de documentación del SGSICN, es obligatorio y atañe a todo el personal de la organización.

4. Aprobación y difusión

Esta Política debe ser revisada anualmente para su adecuación y extraordinariamente cuando concurran situaciones especiales y/o cambios sustanciales en el SGSICN.

Asimismo, la presente versión de la Política es aprobada por la Dirección General, y difundida a toda la Organización, a las partes interesadas y público en general, en Alcorcón el 19 de enero de 2026.