1. Introducción

Afi, consciente de que la seguridad de la información relativa a nuestros clientes es un recurso crítico, ha establecido un Sistema de Gestión de la Seguridad de la Información de acuerdo a los requisitos de la norma ISO/IEC 27001:2013 para garantizar la continuidad de los sistemas de información, minimizar los riesgos de daño y asegurar el cumplimiento de los objetivos fijados.

El objetivo de la Política de Seguridad es fijar el marco de actuación necesario para proteger los recursos de información frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad y disponibilidad de la información.

La eficacia y aplicación del Sistema de Gestión de la Seguridad de la Información es responsabilidad directa del Comité de la Seguridad de la Información, el cual es responsable de la aprobación, difusión y cumplimiento de la presente Política de Seguridad. En su nombre y representación se ha nombrado un Responsable del Sistema de Gestión de la Seguridad de la Información, que posee la suficiente autoridad para desempeñar un papel activo en el Sistema de Gestión de la Seguridad de la Información, supervisando su implantación, desarrollo y mantenimiento.

El Comité de Seguridad de la Información procederá a desarrollar y aprobar la metodología de análisis de riesgos utilizada en el Sistema de Gestión de la Seguridad de la Información.

Toda persona cuya actividad pueda, directa o indirectamente, verse afectada por los requisitos del Sistema de Gestión de la Seguridad de la Información, está obligada al cumplimiento estricto de la Política de Seguridad.

En Afi se implantarán todas las medidas necesarias para cumplir la normativa aplicable en materia de seguridad en general y de seguridad informática, relativa a la política informática, a la seguridad de edificios e instalaciones y al comportamiento de empleados y terceras personas asociadas a Afi en el uso de sistemas informáticos. Las medidas necesarias para garantizar la seguridad de la información mediante la aplicación de normas, procedimientos y controles deberán permitir asegurar la confidencialidad, integridad, disponibilidad de la información, esenciales para:

- Cumplir con la legislación vigente en materia de los sistemas de información.
- Asegurar la confidencialidad de los datos gestionados por Afi.
- Asegurar la disponibilidad de los sistemas de información, tanto en los servicios ofrecidos a los clientes como en la gestión interna.
- Asegurar la capacidad de respuesta ante situaciones de emergencia, restableciendo el funcionamiento de los servicios críticos en el menor tiempo posible.

- Evitar alteraciones indebidas en la información.
- Promover la concienciación y formación en seguridad de la información.
- Establecer objetivos y metas enfocados hacia la evaluación del desempeño en materia de seguridad de la información, así como a la mejora continua en nuestras actividades, reguladas en el Sistema de Gestión que desarrolla esta política.

2. Misión

La misión de Afi se enfoca en brindar información y conocimientos especializados que ayuden a sus clientes a tomar decisiones informadas y estratégicas en el ámbito financiero. Sus áreas de expertise incluyen economía, mercados financieros, banca, seguros, mercados de capitales, análisis de riesgos, entre otros.

3. Marco normativo

El sistema de gestión de seguridad de la información se encamina a definir normas y procedimientos que protejan la información de sus clientes siempre dentro del marco normativo actual de seguridad. En este aspecto, Afi dispone de una documentación interna en la que se describen las normas de aplicación revisadas anualmente, siendo las más relevantes:

- **Ley orgánica 3/2018 de protección de datos personales y garantía de los derechos digitales (LOPDGDD), RD 1720/2007 Desarrollo de la LOPD**
- **Reglamento General de Protección de Datos 2016/679, de 27 de abril de 2016**
- **Ley 34/2002 de servicios de la sociedad de la información y de comercio electrónico(LSSI)**
- **RDL 1/1996 Ley de propiedad intelectual**
- **Ley 17/2001 de propiedad industrial**
- **Ley 1/2019, de 20 de febrero, de Secretos Empresariales.**
- **Reglamento 2022/2554 sobre resiliencia operativa digital en el sector financiero (a partir de 2025)**

4. Modelo de gobernanza

Para garantizar el cumplimiento de esta política y las normativas aplicables se designarán roles de seguridad y constituirá un Comité de Seguridad de la Información

4.1. Roles de seguridad

- Responsable de información
- Responsable de seguridad
- Responsable sistema de gestión
- Responsable de IT

4.2. Comité de seguridad de la información

Se ha constituido un Comité de Seguridad de la Información como máxima autoridad responsable de la gobernanza de la Política de Seguridad de la organización bajo el mando de la comisión ejecutiva.

Los responsables de la Información y de los Servicios serán convocados en función de los asuntos a tratar.
Asimismo, y con carácter opcional, podrán incorporarse a las labores del Comité grupos de trabajo especializados, ya sean de carácter interno, externo o mixto.

4.3. Funciones y responsabilidades

Las funciones y responsabilidades de los roles de seguridad y el comité de seguridad de la información se definen en el Anexo V del manual del sistema gestión en seguridad de la información.

4.4. Designación y renovación

Los roles de seguridad y miembros del comité son designados o revocados por el propio comité de seguridad en decisión tomada por los representantes de la dirección en el comité.

La designación o revocación de los miembros del comité en representación de la dirección serán definidos en la comisión ejecutiva de la organización.

5. Desarrollo de la política de seguridad de la información

El cumplimiento de los objetivos marcados en esta Política de Seguridad se lleva a cabo mediante el desarrollo de documentación que componen las normas y procedimientos de seguridad asociados al cumplimiento de la norma ISO 27001:2013, y en aquellos servicios prestados a las administraciones públicas, también el Esquema Nacional de Seguridad para los niveles de seguridad establecidos en el servicio.

La revisión anual de la presente Política corresponde al Comité de Seguridad de la Información proponiendo en caso de que sea necesario mejoras de la misma, para su aprobación por parte del mismo órgano que la aprobó inicialmente.