

Política Corporativa de Seguridad de la Información

Ed. 02 - Fecha: 26/02/2021



1. Objeto de la política

El Comité de Dirección de ABAI Group reconoce como activos estratégicos la información y los sistemas que la soportan, por lo que manifiesta su determinación en alcanzar los niveles de seguridad necesarios que garanticen su protección.

El objeto de la Política Corporativa de Seguridad de la Información es proporcionar las directrices para garantizar la mejora continua de la seguridad de la información y de la calidad de los servicios que el Grupo ABAI Group ofrece a sus clientes en cada una de sus empresas.

2. Alcance

Esta política abarca a toda la información utilizada por ABAI Group para el desarrollo de sus actividades y es aplicable, con carácter obligatorio, las distintas empresas del Grupo ABAI Group, así como a las entidades colaboradoras involucradas en la utilización de la información y los sistemas.

Las relaciones con dichas entidades colaboradoras deben de estar amparadas siempre por los contratos de prestación de servicios correspondientes, incluyendo cláusulas de garantías en el uso de la información.

La política de seguridad será de aplicación en todas las fases del ciclo de vida de los datos: generación, distribución, almacenamiento, procesamiento, transporte, consulta y destrucción; y de los sistemas que los procesan: análisis, diseño, desarrollo, implantación, explotación y mantenimiento.

Esta política persigue la adopción de acciones destinadas a preservar las cuatro componentes básicas de la seguridad aplicadas a la información:

- Confidencialidad: Garantizar que a los datos y a los sistemas solo accedan personas debidamente autorizadas.
- Integridad: Garantizar la exactitud de la información y de los sistemas contra alteración, pérdida o destrucción, ya sea de forma accidental o fraudulenta.
- Disponibilidad: Garantizar que la información y los sistemas pueden ser utilizados en la forma y tiempo requeridos.
- Trazabilidad: Garantizar que cualquier acción o transacción pueda ser relacionada unívocamente asegurando el cumplimiento de controles claves establecidos en las correspondientes normativas.

3. Marco jurídico

ABAI Group adquiere el compromiso de velar por el cumplimiento de la legislación vigente en materia de protección y seguridad de la información y de los sistemas aplicable a todos sus procesos de negocio en aquellos países en los que opere.

4. Organización y responsabilidades

La función de seguridad reside en el Comité Corporativo de Seguridad. Con dependencia funcional y autoridad delegada de éste, el responsable de seguridad de la información y el responsable de seguridad física canalizan las directrices y normativas hacia las distintas empresas del Grupo ABAI.

El Comité Corporativo de Seguridad establece y tutela los Subcomités de Seguridad en cada país donde opera ABAI, y los Subcomités Corporativos que considere necesarios, en los que delega la gestión de la seguridad de temas específicos.

Las organizaciones usuarias y de soporte, en cumplimiento de las normativas de seguridad, implantarán los controles necesarios asistidos por la organización de seguridad corporativa y local del país.

La dirección de tecnología es la responsable de la seguridad de plataformas, redes e infraestructura de tratamiento de la información, dando servicio a las demás direcciones del Grupo ABAI Group propietarias y/o depositarias de la información, conforme a las necesidades de seguridad que estas demanden de acuerdo a las normativas establecidas y requerimientos de los clientes.

Todo usuario de los sistemas es responsable del uso adecuado que haga de los mismos y de cumplir con las obligaciones y los controles establecidos.

5. Clasificación de la información

Toda información deberá estar clasificada en virtud de su importancia para la organización y ha de ser tratada según dicha clasificación, acorde a lo dispuesto en la normativa sobre clasificación y tratamiento de la información.

6. Aplicación de la política de seguridad

Con objeto de poder aplicar las líneas de actuación expuestas en esta política, se precisa la definición, elaboración, implantación y mantenimiento de planes de seguridad y de continuidad, tanto de ámbito corporativo como en cada empresa del Grupo, donde se recojan:

- El conjunto de normativas, estándares, guías y procedimientos operativos que determinen la forma adecuada de actuar en materia de seguridad.
- Los proyectos de inversión que doten de medios necesarios para la consecución de estos objetivos.
- Las organizaciones responsables de gestionar la seguridad en sus distintos aspectos.
- Los métodos de control, revisión y ajuste que permitan verificar el correcto funcionamiento de los planes de seguridad y continuidad.

La elaboración de los planes de seguridad y continuidad deberá acompañarse de procesos formales de análisis y gestión de riesgos que permitan implantar las soluciones idóneas, o bien asumir los riesgos asociados a las desviaciones respecto de estas soluciones.

7. Formación y concienciación

El método más efectivo de mejorar la seguridad es mediante la formación continuada y su incorporación a la actividad laboral.

Dentro de los planes de formación se incluirán cursos específicos sobre seguridad de la información acorde con el área destinataria: Dirección, técnicos, administradores y usuarios de los sistemas. Así mismo se realizarán campañas de medio que se considere más efectivo.

8. Auditoría

Los sistemas de información se someterán periódicamente a auditorías internas o externas con la finalidad de verificar el correcto funcionamiento de los planes de seguridad, determinando grados de cumplimiento y recomendando medidas correctoras.

9. Planes específicos

Cualquier plan específico sobre seguridad deberá ajustarse a las disposiciones y recomendaciones de carácter más general y superior del presente documento.

10. Efectividad

La Política Corporativa de Seguridad de la Información entrará en vigor desde el mismo día de su publicación.

