Alaiant

POLÍTICA CORPORATIVA

Política de Seguridad de la Información y Protección de Datos

Alaiant Valores, S.V., S.A.

TIPO DE DOCUMENTO	ENTIDAD	PÁGINAS
Política corporativa	Alaiant Valores, S.V., S.A.	5

Índice

1) Declaración y propósito..... 3
2) Alcance..... 3
3) Marco normativo..... 3
4) Principios rectores..... 3
5) Compromisos de seguridad y privacidad..... 3
6) Gobernanza y responsabilidades..... 4
7) Privacidad y protección de datos personales..... 4
8) Cumplimiento y disciplina..... 4
9) Comunicación, revisión y vigencia..... 4

RIESGOS Y POLÍTICAS

Política de seguridad de la información y protección de datos

Alaiant Valores, S.V., S.A.

1) Declaración y propósito

La presente Política establece los principios y compromisos mediante los cuales ALAIANT VALORES, SOCIEDAD DE VALORES, S.A. (Alaiant) protege su información y servicios, reconociendo su carácter estratégico y la necesidad de garantizar su confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad para salvaguardar la continuidad del negocio.

2) Alcance

Aplica a todas las personas que accedan, traten o custodien información de Alaiant (empleados, directivos, colaboradores y terceras partes), así como a todos los sistemas, medios y tecnologías utilizados para su procesamiento, almacenamiento o transmisión, con independencia del formato (físico o digital).

3) Marco normativo

Alaiant cumple y se compromete a demostrar cumplimiento con la normativa aplicable, entre otras: RGPD (UE) 2016/679, LOPDGDD 3/2018, Reglamento (UE) 2022/2554 (DORA) y demás requisitos legales, regulatorios o contractuales que resulten de aplicación.

4) Principios rectores

- Enfoque basado en riesgos: la seguridad se gestiona mediante identificación, evaluación y tratamiento de riesgos, manteniéndolos dentro de niveles tolerables aprobados por el Consejo de Administración.
- Proporcionalidad y “seguridad por diseño y por defecto” en procesos y tecnologías.
- Mejora continua: revisión, auditoría y actualización periódica del sistema de gestión.
- Clasificación y protección de activos según criticidad y sensibilidad de la información.

5) Compromisos de seguridad y privacidad

1. Proteger la información y los servicios frente a pérdidas de disponibilidad, integridad y confidencialidad, así como a preservar autenticidad y trazabilidad.
2. Definir y aplicar controles preventivos, de detección, respuesta y recuperación acordes a la criticidad y clasificación de los activos.

3. Realizar análisis y gestión de riesgos periódicos, y aprobar los riesgos residuales y planes de tratamiento correspondientes.
4. Gestionar incidentes de seguridad (detección, clasificación, contención, erradicación, recuperación y lecciones aprendidas), incluyendo las notificaciones regulatorias cuando proceda.
5. Asegurar la continuidad y resiliencia operativa, con copias de respaldo, pruebas de restauración y planes de continuidad/recuperación adecuados.
6. Aplicar cifrado y controles de acceso apropiados para la protección de datos en reposo y en tránsito, e implantar registros de actividad para asegurar la trazabilidad.
7. Integrar la seguridad y la privacidad en el ciclo de vida de los sistemas (adquisición, desarrollo, cambios y retirada).
8. Concienciar y formar de manera periódica a empleados y colaboradores sobre sus responsabilidades.
9. Garantizar la protección de datos personales mediante la aplicación de medidas técnicas y organizativas apropiadas, asegurando el cumplimiento del RGPD y la LOPDGDD en todos los procesos de tratamiento.
10. Exigir a terceros y proveedores niveles de seguridad equivalentes, mediante cláusulas y controles de supervisión.

6) Gobernanza y responsabilidades

El Consejo de Administración lidera la seguridad de la información, asigna recursos y aprueba el nivel de tolerancia al riesgo. Se designan las funciones clave —Responsable de Seguridad, Responsable del Sistema y Delegado/a de Protección de Datos (DPO)— y se establece un Comité de Seguridad, Privacidad y Protección de Datos para coordinar la estrategia, el seguimiento de riesgos y la mejora continua del sistema de gestión.

7) Privacidad y protección de datos personales

Cuando exista tratamiento de datos personales, Alaiant observa los principios de licitud, lealtad y transparencia; limitación de la finalidad; minimización; exactitud; limitación de conservación; e integridad y confidencialidad, aplicando medidas técnicas y organizativas apropiadas (art. 32 RGPD) y los principios de privacidad desde el diseño y por defecto.

8) Cumplimiento y disciplina

El incumplimiento de esta política y sus normas de desarrollo podrá conllevar medidas disciplinarias internas y/o las acciones contractuales y legales que procedan en el caso de terceros.

9) Comunicación, revisión y vigencia

Esta política es pública, se comunica a las partes interesadas y se revisará al menos anualmente o ante cambios relevantes del entorno, de los riesgos o del marco normativo.

Las políticas y procedimientos derivados desarrollan los aspectos operativos y técnicos de su cumplimiento.