1. DECLARACIÓN DE COMPROMISO

SMART SOFT COLOMBIA S.A.S. entendiendo la importancia de la seguridad de la información relacionada con sus servicios de innovación y consultoría en el desarrollo de software para sus clientes, se ha comprometido a gestionar la presente política y los objetivos de seguridad de la información. Por ello, establece un marco de confianza, en concordancia con la misión, visión y objetivos de la Compañía e implementa las mejores prácticas para garantizar la gestión de los riesgos de seguridad de la información que permitan preservar la confidencialidad, integridad y disponibilidad de los activos de información. Para esto, se apoya en la gestión integral de los riesgos, el compromiso de sus funcionarios y la alta gerencia para el cumplimiento de los requisitos legales, contractuales y reglamentarios, y, en la búsqueda permanente de la mejora continua.

2. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

SMART SOFT COLOMBIA S.A.S. empresa privada, con personería jurídica, autonomía administrativa y patrimonio independiente, consciente de la importancia que la seguridad de la información tiene para el desarrollo y buen funcionamiento de sus procesos internos, ha decidido implementar un Sistema de Gestión de Seguridad de la Información (SGSI), basado en la norma internacional ISO 27001:2022, por medio de la definición y adopción de la presente política.

SMARTSOFT establece, define y revisa sus objetivos, dentro del SGSI, encaminados a mejorar la seguridad de su información de sus procesos para la prestación de servicios relacionados con el desarrollo de software. Esta, se entiende como la preservación de la confidencialidad, integridad y disponibilidad de la información, así como de los sistemas que la soportan, lo que incrementa los niveles de confianza en los colaboradores, clientes y partes interesadas. Todo lo anterior fortalecido mediante el cumplimiento de los requisitos legales, reglamentarios y contractuales que le sean aplicables.

La Alta Dirección se compromete a la implantación, mantenimiento y mejora de la política, dotándola, en el marco de la implementación del SGI, de aquellos medios y recursos que sean necesarios e instando a todos los colaboradores, proveedores y partes interesadas para que asuman este compromiso. Para ello, definirá las medidas requeridas para la formación y concienciación de sus grupos de interés.

3. OBJETIVO GENERAL

La presente Política de Seguridad de la Información tiene como objetivo definir los lineamientos generales para garantizar la gestión, protección y funcionamiento de los activos de información de SMARTSOFT, así como promulgar la operación del SGSI en los procesos internos y dentro del alcance de los proyectos que desarrolla la Compañía,

con el fin de preservar la disponibilidad, integridad y confidencialidad de la información y el aseguramiento de la continuidad del negocio.

4. OBJETIVOS ESPECÍFICOS

a) Definir, implementar y mantener un Sistema de Gestión de Seguridad de la Información que permita gestionar los riesgos de seguridad de la información transversales a los procesos del negocio en alineación con los objetivos estratégicos de la organización.

b) Implementar controles técnicos y administrativos apropiados para proteger los activos de información, basados en los resultados del análisis de riesgos. Esto incluye la adopción de buenas prácticas para proteger los activos de información, con base en los criterios de confidencialidad, integridad y disponibilidad.

c) Sensibilizar y capacitar a los empleados y partes interesadas sobre las políticas y directrices definidas en el Sistema de Gestión de Seguridad de la Información, las mejores prácticas en el desarrollo seguro de software, así como crear conciencia sobre las amenazas y riesgos potenciales.

d) Monitorear el cumplimiento de los requisitos legales y reglamentarios aplicables al desarrollo del propósito de SMARTSOFT para garantizar que el desarrollo de software cumpla con las leyes y regulaciones aplicables relacionadas con la privacidad de datos, la protección de la información y otras áreas relevantes.

e) Establecer procedimientos claros y eficientes para detectar y responder a incidentes de seguridad, incluyendo la notificación adecuada a las partes interesadas y la evaluación de los impactos.

f) Realizar mínimo una vez al año revisiones del SGSI para asegurar su adecuación, suficiencia y eficacia, ajustándolo a las necesidades cambiantes del negocio, el entorno tecnológico y el panorama de amenazas.

5. ALCANCE

La Política de Seguridad de la Información cubre los activos de información críticos de todos los procesos de la organización y es aplicable a todos los funcionarios, contratistas y terceros. El límite de la política se establece para los procesos internos de SMARTSOFT y de ninguna manera remplaza una Ley o requisito reglamentario aplicable a la organización.

6. ROLES Y RESPONSABILIDADES CON LA SEGURIDAD DE LA INFORMACIÓN

La implementación efectiva de esta política es responsabilidad de todos los miembros de la organización. El Oficial de Seguridad de la Información es responsable de velar por el cumplimiento y el mantenimiento de esta política. Los líderes de cada proceso deben asegurar que sus equipos de trabajo cumplan con los principios y directrices definidos en esta política y en las políticas específicas. Los roles y responsabilidades del SGSI han sido establecidos en la descripción de los roles corporativos.

7. VIGENCIA

Esta política es aplicable para todos los funcionarios, contratistas y terceros a partir de momento de su publicación, será revisada anualmente y actualizada según corresponda y comunicada por los medios establecidos por la Organización a todos los trabajadores y partes interesadas.

8. DECLARACIÓN DE MEJORA CONTINUA

- La organización se compromete a mantener una cultura de mejora continua en todos los aspectos de la gestión de la seguridad de la información.
- Se deben llevar a cabo revisiones periódicas y sistemáticas de las políticas de seguridad de la información, evaluando su efectividad y relevancia en el contexto de las amenazas y los riesgos emergentes.
- Se implementa un ciclo de mejora continua, basado en el modelo PHVA.
    - **Planificar:** Identificar áreas de mejora, establecer objetivos de seguridad y desarrollar planes para alcanzar esos objetivos.
    - **Hacer:** Implementar los cambios planificados y las nuevas medidas de seguridad.
    - **Verificar:** Monitorear y evaluar la eficacia de las implementaciones, identificando oportunidades para mejoras adicionales.
    - **Actuar:** Implementar acciones correctivas basadas en las evaluaciones y volver a planificar para mejoras continuas.
- Se debe promover la formación continua y la sensibilización del personal sobre las mejores prácticas en seguridad de la información.
- La retroalimentación de los incidentes de seguridad y de las auditorías internas y externas será utilizada como una fuente valiosa para la mejora del SGSI.
- La alta dirección apoyará y facilitará los recursos necesarios para la mejora continua y el desarrollo del personal en áreas críticas de seguridad de la información.

9. CONSECUENCIA DE INCUMPLIMIENTO

Cualquier violación o incumplimiento a la presente política es calificada como grave y constituye justa causa para dar por terminado el contrato laboral o contractual vigente.

PEDRO ELÍAS PABÓN LOZANO
Gerente General

ELABORÓ	REVISÓ	APROBÓ
Samuel Córdoba Jiménez **CISO**	Johely Lorena López A. **Gerente Administrativa y Financiera**	Pedro Pabón **Gerente General**

CONTROL DE CAMBIOS

VERSIÓN	OBSERVACIÓN	FECHA
1.0	Creación del documento.	22/01/2021
2.0	Actualización general de la política y redefinición de los objetivos específicos.	4/2/2024
3.0	Adición y definición de Roles y responsabilidades. Declaración de la mejora continua.	12/06/2024
4.0	Aclaración de la periodicidad respecto del numeral f de los objetivos específicos. Revisión de etiquetado.	16/05/2025