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

1. DECLARACIÓN DE COMPROMISO

SMART SOFT COLOMBIA S.A.S. reconoce que la protección de la información es esencial para mantener la confianza de nuestros clientes y garantizar la continuidad del negocio. Esta política establece los requisitos mínimos de seguridad que deben cumplir los proveedores que interactúen con información o activos de información, conforme con el Sistema de Gestión de Seguridad de la Información (SGSI) basado en la NTC ISO/IEC 27001:2022.

2. ALCANCE

Esta política aplica a todos los proveedores que tengan acceso, procesen, custodien o gestionen información de SMART SOFT COLOMBIA S.A.S. o de sus clientes, en cualquier formato (electrónico, físico, nube u otro medio), incluyendo servicios de desarrollo de software, soporte, infraestructura TIC, aplicaciones, bases de datos y demás activos relacionados.

3. POLÍTICA GENERAL

Todos los proveedores deben implementar medidas que aseguren la confidencialidad, integridad y disponibilidad de la información. Estas medidas deben ser coherentes con los requisitos contractuales, el nivel de riesgo asociado y las mejores prácticas internacionales de seguridad.

Los acuerdos contractuales deberán reflejar las responsabilidades en seguridad de la información y permitir a SMART SOFT COLOMBIA S.A.S. auditar su cumplimiento.

4. REQUISITOS DE CUMPLIMIENTO

Los proveedores deberán:

a) Contar con una Política de Seguridad de la Información, aprobada por su alta dirección, alineada con los principios de la NTC ISO/IEC 27001.
b) Fomentar una cultura de seguridad de la información, de forma que realice capacitaciones periódicas a su personal en temas de ciberseguridad y gestión de incidentes.

c) Gestionar los riesgos de seguridad de la información relacionados con los servicios prestados, incluyendo los asociados al diseño y desarrollo de software. Además, deberán documentar y aplicar controles para mitigar los riesgos identificados, en los casos que aplique.
d) Implementar controles de acceso que aseguren que solo personal autorizado acceda a la información y a los entornos de desarrollo, pruebas y producción. Los accesos deben revisarse y auditarse mínimo una vez al año.
e) Gestionar los activos de información, identificándolos, clasificándolos y protegiéndolos contra accesos no autorizados, alteraciones y pérdida.
f) Contar con un procedimiento formal de gestión de incidentes de seguridad, el cual contemple notificar de manera inmediata a SMART SOFT COLOMBIA S.A.S. sobre cualquier incidente que afecte información, sistemas o servicios provistos.
g) Someterse a seguimiento y revisión de servicios y cambios que afecten la seguridad, incluyendo nuevas tecnologías, subcontratistas, ambientes de desarrollo, cambios de ubicación, nuevas aplicaciones y actualizaciones. Todo cambio deberá ser evaluado y aprobado por SMART SOFT COLOMBIA S.A.S.

Para garantizar que los servicios ofrecidos se mantengan seguros y eficientes, el Proveedor deberá contar con parámetros mínimos de seguridad de la información que se ajusten a los principios de la norma técnica ISO 27001:2022 y en función al tipo de relación comercial que tengan con SMART SOFT COLOMBIA S.A.S. Todos los proveedores deberán haber contar, como mínimo, con el Acuerdo de Seguridad de la Información para Proveedores, definido por la Organización.

5. SEGURIDAD EN LA CADENA DE SUMINISTRO TIC

Para las relaciones comerciales involucradas en el diseño, fabricación, distribución y soporte de productos y servicios TIC (Tecnologías de la Información), incluyendo hardware, software y servicios, dichos proveedores deberán:

- Identificar, documentar y garantizar su cadena de suministro, así como el cumplimiento de los requisitos relacionados con la implementación de las prácticas de seguridad de la información.
- Evaluar los riesgos de seguridad, privacidad y operacionales de los terceros involucrados.
- Asegurar la seguridad en el ciclo de vida del software, incluyendo pruebas de vulnerabilidades, gestión de dependencias, validación de librerías y controles en los pipelines de integración y despliegue continuo (CI/CD).

6. AUDITORÍAS Y EVALUACIONES

SMART SOFT COLOMBIA S.A.S. podrá realizar auditorías periódicas, remotas, para verificar el cumplimiento de esta política. Los proveedores deberán permitir el acceso a la documentación y suministrar las evidencias relevantes.

7. VIGENCIA Y REVISIONES

Esta política entra en vigor desde su publicación y será revisada al menos anualmente. Cualquier actualización será notificada a los proveedores mediante los canales oficiales establecidos por SMART SOFT COLOMBIA S.A.S.

8. CONSECUENCIAS DE INCUMPLIMIENTO

El incumplimiento de esta política constituye una falta grave y podrá derivar en la terminación del contrato, así como en la exigencia de reparación por los daños ocasionados.

Este documento forma parte integral del SGSI de SMART SOFT COLOMBIA S.A.S y se alinea con los controles y directrices de la NTC ISO/IEC 27001:2022.

PEDRO ELÍAS PABÓN LOZANO
Gerente General

CONTROL DE CAMBIOS

VERSIÓN	OBSERVACIÓN	FECHA
3.0	Se revisa y ajusta la totalidad del texto de la Política como acción correctiva de la ncm #7 de la auditoría de otorgamiento en ISO 27001:2022, para alinear las directrices de la política con los requisitos de Seguridad de la Información pertinentes a cada proveedor y la operación.	01/07/2025
2.0	Se ajusta la etiqueta del documento.	16/05/2025
1.0	Creación del documento.	11/06/2024