Tabla de Contenido

1. Introducción

El creciente uso de información ha potenciado la agilidad y escalamiento de los procesos en las empresas, en esta misma proporción enfrentan riesgos procedentes de una amplia variedad de amenazas que pueden afectar de forma critica la información y sus recursos de procesamiento, almacenamiento y transmisión, en pro de enfrentar estas circunstancias, **INALAMBRIA INTERNACIONAL** establece estrategias y controles adecuados, que promueven una gestión segura de los procesos y permiten brindar mayor protección a la información, es por ello, que estas estrategias y lineamientos para la protección y control parten de marcos normativos establecidos, que deben ser desarrollados para realizar una gestión adecuada.

INALAMBRIA INTERNACIONAL ha reconocido la información como un activo vital en su organización, de esta forma, y con el fin de mitigar los riesgos y proteger la información, implementa un conjunto de controles, lineamientos y procedimientos para alcanzar un nivel apropiado de seguridad de la información, así como los mecanismos para administrar, mantener y mejorar los controles a lo largo del tiempo.

2. Política General Seguridad de la Información y Ciberseguridad

INALAMBRIA INTERNACIONAL, se compromete a preservar la confidencialidad, disponibilidad e integridad de sus activos de información o que por sus funciones mantenga como custodio, protegiéndolos contra amenazas internas y externas, mediante el sistema de gestión de seguridad de la información en conformidad con el estándar ISO 27001 vigente y la metodología para la gestión del riesgo, manteniendo la mejora continua; adicionalmente a cumplir con las disposiciones constitucionales y legales aplicables, así como las disposiciones internas, relacionadas con la seguridad de la información.

Para tal fin, la dirección de **INALAMBRIA INTERNACIONAL** en su actividad y gestión está comprometida en velar por la seguridad de la información y ciberseguridad, garantizando la protección de la información e identificando las amenazas con el fin de asegurar la continuidad del negocio y la pronta respuesta a los incidentes.

De acuerdo con lo anterior, se establecen 8 principios de seguridad que dan soporte a esta política de INALAMBRIA:

- **INALAMBRIA INTERNACIONAL** ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios que le aplican a su naturaleza.

- Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, proveedores y terceros.

- **INALAMBRIA INTERNACIONAL** protegerá la información generada, procesada o resguardada por los procesos de negocio, su infraestructura tecnológica y activos del riesgo que se genera de los accesos otorgados a terceros; proveedores o clientes.

- Inalambria protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales, mediante la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en su custodia

- **INALAMBRIA INTERNACIONAL** garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información

- **INALAMBRIA INTERNACIONAL** garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.

- **INALAMBRIA INTERNACIONAL** garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

Por lo tanto, se establecen los siguientes objetivos del Sistema de Gestión de Seguridad de la Información:

Objetivo General del SGSI: Fortalecer la disponibilidad, confidencialidad e integridad de información en INALAMBRIA INTERNACIONAL, mediante la implementación de medidas y lineamientos de seguridad y de continuidad en sus operaciones.

Objetivos Específicos del SGSI:

- Gestionar los recursos en seguridad de la información de tal manera que se realice un adecuado uso de los activos de información.

- Asegurar la disponibilidad, confidencialidad e integridad de los servicios prestados por **INALAMBRIA INTERNACIONAL**

- Mitigar los riesgos a activos de información que puedan causar daño a la organización.

- Establecer una cultura en seguridad de la información mediante el desarrollo permanente de los colaboradores.

- Diseñar, implementar, mantener y mejorar de manera continua un Sistema de Gestión de Seguridad de la Información.

Esta política, será revisada anualmente, comunicada, y debe estar accesible a clientes, proveedores y colaboradores y a las demás partes interesadas.

3. Alcance/ Aplicabilidad

Esta política aplica a toda **INALAMBRIA INTERNACIONAL**; personal, contratistas y terceros.

4. Nivel de cumplimiento

Todas las personas cubiertas por el alcance y aplicabilidad deberán dar total cumplimiento de la Política General de Seguridad de la Información y Ciberseguridad de Inalambria.

La presente Política General de Seguridad de la Información y Ciberseguridad entra en vigencia una vez oficializada por Gerencia General de **INALAMBRIA INTERNACIONAL** y, los Responsables de Procesos serán responsables de ponerlas en conocimiento de sus equipos.

Para el caso del personal que se contrate con posterioridad a la fecha de publicación, se le deberá´ entregar una copia del presente documento y hacer firmar una declaración de toma de conocimiento y aceptación de la misma.

El incumplimiento a la Política General de Seguridad de la Información y Ciberseguridad, traerá consigo, las consecuencias legales que apliquen al Reglamento Interno de Inalambria, incluyendo las reglamentaciones que competen al Gobierno Nacional en cuanto a Seguridad y Privacidad de la Información.

4.1 Mantención de la política

- La mantención de la presente política será realizada por el Comité de Gerencia y sus cambios aprobados por Gerencia General de **INALAMBRIA INTERNACIONAL**.

- Las políticas específicas asociadas a la presente política general deberán ser aprobadas y firmadas por Gerencia General. Los procedimientos asociados serán aprobados por Comité de Gerencia.

- El presente documento debe ser revisado a lo menos 1 vez al año y actualizado cada vez que se realicen cambios relevantes en **INALAMBRIA INTERNACIONAL** que afecten la adecuada

protección de la información, considerando como tales entre otros, cambios en la misión, objetivos estratégicos, productos estratégicos, infraestructura, personal y/o procedimientos relacionados con la protección de la información.

4.2 Documentación de Referencia

El presente documento constituye una política de alto nivel, destinada a normar los aspectos más relevantes de la gestión de seguridad de la información, con una vigencia de largo plazo, por lo cual la Dirección promulgará documentos adicionales que explicitan en mayor detalle las medidas de seguridad de alto nivel dispuestas en el presente documento.

Dichos documentos deben estar asociados a los objetivos de control definidos en la ISO/IEC 27001:2022, estos son:

- Políticas Específicas de Seguridad de la Información y Ciberseguridad con aspectos relacionados a controles organizacionales, de Personas, Físicos y Tecnológicos.
- Procedimientos, manuales, instructivos, reglamentos entre otros.

CONTROL DE CAMBIOS			
REV Nº	Descripción del cambio	Aprobado por	Fecha
1	Creación del documento	Representante Legal	Nov 06/2020
2	Actualización documento	Representante Legal	Mar 09/2022
3	Versión 2 de documento	Gerencia General	En 16/2023

Firmas de control

Elaboró:	Revisó:	Aprobó:
Paula A. Hurtado Oficial de Seguridad de la Información -ISO-	Agustín Vélez Mile Castaño Carlos Sierra Comité de Gerencia	Agustín Vélez Presidente Junta Directiva Gerencia General

Documento aprobado mediante proceso de autorización digital. No requiere firma física.