1. Objetivo

La Política de Seguridad de la Información establece el compromiso de NovaSec SAS con la protección y gestión eficiente de sus activos de información, incluidos integrantes, contratistas, terceros, datos, procesos, sistemas y tecnologías (hardware y software) que respaldan sus operaciones y objetivos estratégicos. Esta política busca garantizar un entorno seguro y confiable para el ejercicio de sus actividades y el cumplimiento de los compromisos adquiridos con sus clientes, asegurando la alineación con las normativas vigentes, así como con la misión y visión de la organización.

Para lograr lo anterior, la Alta Dirección se compromete a:

- Implementar un Modelo de Gestión de Seguridad de la Información (SGSI) que asegure la confidencialidad, integridad y disponibilidad de los activos críticos.
- Asignar responsabilidades claras para la gestión de la seguridad, asegurando que todas las partes involucradas (internas y externas) comprendan su rol en la protección de la información.
- Identificar y gestionar de manera sistemática los riesgos relacionados con la información, minimizando el impacto de posibles incidentes y manteniendo un nivel de exposición controlado.
- Fomentar una cultura de seguridad mediante la capacitación continua y la sensibilización del personal en temas de seguridad de la información y ciberseguridad.
- Responder ágilmente a eventos e incidentes de seguridad para proteger los activos de información y mitigar cualquier daño potencial.
- Promover la mejora continua mediante la revisión periódica de los controles, políticas y procedimientos de seguridad, garantizando su actualización conforme a las necesidades del negocio y los cambios normativos.

Esta política refleja el compromiso de NovaSec SAS de establecer un marco de confianza y resiliencia, respaldado por controles de seguridad adecuados, que respalden el cumplimiento de sus objetivos organizacionales y las expectativas de sus clientes.

2. Alcance

Esta política general se aplica a toda la organización, incluyendo integrantes, contratistas, proveedores, terceros, y clientes que gestionen, procesen o tengan acceso a cualquier tipo de información de NovaSec SAS. Abarca todos los sistemas de información, dispositivos, redes, aplicaciones y servicios utilizados para procesar, almacenar o transmitir información, así como todas las ubicaciones físicas y virtuales donde la organización opera.

El alcance incluye:

- Toda la información crítica de la organización, como información financiera, personal, confidencial, propietaria y comercial, así como la de sus clientes y partes interesadas.
- Procesos, procedimientos y actividades asociados con la gestión de la información y su protección a lo largo de todo su ciclo de vida, desde su creación, uso, almacenamiento y transmisión, hasta su eliminación o destrucción segura.
- Todas las fases operativas y niveles de la organización, garantizando que cada persona comprendida en este alcance cumpla plenamente con los lineamientos y controles establecidos en esta política.

La política se extiende a cualquier tecnología de la información que respalde los procesos organizacionales, tanto propiedad de la organización como aquellas gestionadas por terceros. Toda persona o entidad cubierta por este alcance tiene la responsabilidad de adherirse al 100% a las directrices establecidas en esta política, contribuyendo al objetivo de mantener un entorno seguro y resiliente.

3. Declaraciones

Para garantizar la protección integral de los activos de información y el cumplimiento de los objetivos organizacionales, **NovaSec SAS** se compromete a:

3.1. Compromiso y Marco de Referencia

- Adoptar la norma ISO/IEC 27001:2022 como marco de referencia para implementar, operar y mejorar continuamente su Sistema de Gestión de Seguridad de la Información (SGSI).
- Alinear las políticas, procedimientos e instructivos con las necesidades organizacionales y los requisitos regulatorios y contractuales aplicables.

3.2. Protección de Información y Gestión de Riesgos

- Proteger la información generada, procesada, almacenada o transmitida por sus procesos de negocio, minimizando impactos financieros, operativos y legales ante cualquier incidente.
- Implementar controles basados en la clasificación de la información, según su criticidad y sensibilidad, garantizando la aplicación de medidas proporcionales al riesgo.
- Gestionar de manera proactiva los riesgos de seguridad de la información, priorizando la protección contra accesos no autorizados, pérdidas, robos, daños o divulgaciones indebidas.

3.3. Seguridad Integral en Procesos y Tecnología

- Asegurar la protección de las instalaciones y la infraestructura tecnológica que soportan procesos críticos de negocio.
- Controlar el acceso a los sistemas, redes y recursos tecnológicos, asegurando que solo los usuarios autorizados accedan a la información necesaria para sus funciones.
- Incorporar la seguridad en todo el ciclo de vida de los sistemas de información, desde su diseño hasta su eliminación.

3.4. Cultura Organizacional y Responsabilidades

- Fomentar una cultura de seguridad de la información mediante la capacitación continua y la concienciación de todos los integrantes, contratistas y terceros.
- Asignar y comunicar responsabilidades claras para la gestión de la seguridad, asegurando la aceptación de los roles y tareas asignadas.

3.5. Gestión de Incidentes y Continuidad del Negocio

- Monitorear y auditar regularmente los sistemas y procesos, garantizando la detección temprana y respuesta efectiva ante incidentes de seguridad de la información.

- Implementar una adecuada gestión de eventos y debilidades, promoviendo la mejora continua del modelo de seguridad.
- Garantizar la disponibilidad y continuidad de los procesos de negocio esenciales, minimizando el impacto de interrupciones operativas.

3.6. Cumplimiento Legal y Consecuencias por Incumplimiento

- Cumplir con todas las leyes, normativas y regulaciones nacionales e internacionales relacionadas con la seguridad y privacidad de la información.
- Adoptar medidas legales y disciplinarias en caso de incumplimiento de las políticas de seguridad, de acuerdo con las normativas internas y las leyes vigentes.

4. Aprobación

	Elaboró	Revisó	Aprobó
Nombre	Oscar Ardila	Miguel Palma	Alvaro Trujillo
Cargo	Consultor NewNet	Gerente de Servicios	Gerente
Fecha	Octubre 30 de 2024	Noviembre 1 de 2024	Noviembre 1 de 2024

5. Control de Cambios

Fecha	Modificado por	Versión	Referencia del cambio
Febrero 28 de 2023	Sergio Lubo	1.0	Versión Inicial
Octubre 30 de 2024	Oscar Alfonso Ardila Jimenez	2.0	Versión de actualización marco

			ISO 27001:2022