I. OBJETIVO

Establecer los lineamientos para la gestión segura de la información institucional, garantizando la confidencialidad, integridad y disponibilidad de los activos de información, así como el cumplimiento de la normativa vigente en materia de protección de datos personales, a través de la educación de los trabajadores, para lograr personal competente y comprometido con una cultura de seguridad de la información reflejada en la aceptación y aplicación de las directrices de seguridad.

II. ALCANCE

Esta política aplica a todos los colaboradores, contratistas, proveedores y terceros que accedan, procesen, almacenen o gestionen información de la organización, incluyendo datos personales de clientes, pacientes, empleados y aliados estratégicos.

III. MEDIDAS PARA GARANTIZAR LA SEGURIDAD DE LA INFORMACIÓN

NEW BIOLOGY S.A.S. garantizará la protección de los activos de información (trabajadores, usuarios, pacientes, historia clínica, los procesos, las tecnologías de información incluido el hardware y el software), a través de mecanismos de tratamiento, almacenamiento y comunicación donde están contenidos y soportados sus servicios de consulta, registro, validación y realización de trámites , contando con personal competente y comprometido con una cultura de seguridad reflejada en la aceptación y aplicación de las directrices establecidas. Con la implementación de políticas en seguridad de la información, se busca dar cumplimiento a disposiciones legales y regulatorias emitidas por los diferentes organismos estatales, contar con una metodología de gestión de riesgos como herramienta para actuar proactivamente ante la presencia de situaciones que puedan afectar la continuidad de los procesos de **NEW BIOLOGY S.A.S.**

IV. PRINCIPIOS RECTORES.

La seguridad de la información se fundamenta en tres principios esenciales:

1. **CONFIDENCIALIDAD:** Para garantizar que la información solo sea accesible a personas autorizadas.
2. **INTEGRIDAD:** Asegurar que los datos no sean modificados sin autorización.
3. **DISPONIBILIDAD:** Permite que la información esté accesible cuando se requiera para el cumplimiento de las funciones institucionales.

Estos principios se complementan con el respeto por la legalidad, la responsabilidad proactiva y el uso ético de los recursos tecnológicos.

V. CLASIFICACIÓN DE LA INFORMACIÓN

La información institucional se clasifica según su nivel de sensibilidad y criticidad. Se considera **información pública** aquella que puede ser divulgada sin restricciones; **información interna**, la que es de uso exclusivo dentro de la organización; **información confidencial**, aquella que requiere protección especial por su naturaleza estratégica o sensible; y **datos personales**, que son aquellos que identifican o pueden identificar a una persona natural y cuyo tratamiento debe realizarse conforme a la legislación vigente en materia de protección de datos Ley 1581 de 2012.

VI. PROTECCIÓN DE DATOS PERSONALES

La organización se compromete a garantizar el tratamiento adecuado de los datos personales, conforme a lo establecido en la Ley 1581 de 2012 y demás normas aplicables. Para ello, se recolecta únicamente la información necesaria para fines legítimos, específicos y explícitos, previa autorización del titular. Se garantiza el respeto por los derechos de los titulares, incluyendo el acceso, la rectificación, la cancelación y la oposición al tratamiento de sus datos. Además, se implementan medidas técnicas y administrativas para proteger los datos durante su almacenamiento, transmisión y eliminación, y se prohíbe su cesión a terceros sin las garantías legales correspondientes.

VII. USO DE RECURSOS INFORMÁTICOS

El uso de los recursos informáticos institucionales está restringido a fines laborales y debe realizarse conforme a los principios de legalidad, ética y responsabilidad. Se prohíbe expresamente el uso indebido de la información, la instalación de software no autorizado, el acceso no permitido a sistemas o bases de datos, y cualquier conducta que comprometa la seguridad de los activos tecnológicos o de la información. Las acciones que contravengan esta política podrán ser objeto de sanciones disciplinarias o contractuales, según corresponda.

VIII. GESTIÓN DE INCIDENTES

La organización cuenta con un procedimiento formal para la gestión de incidentes de seguridad de la información. Todo evento que represente una amenaza o vulneración debe ser reportado de inmediato al área responsable, la cual activará los protocolos de respuesta, contención, análisis y mitigación, garantizando la trazabilidad del incidente y la implementación de acciones correctivas y preventivas.

IX. ROLES Y RESPONSABILIDADES

Los roles en materia de seguridad de la información están claramente definidos. Cada usuario es responsable de proteger la información a la que accede y de cumplir con las políticas establecidas. El área de tecnología tiene la función de implementar y mantener los controles técnicos necesarios, mientras que el responsable de protección de datos vela por el cumplimiento de la normativa vigente y actúa como punto de contacto para los titulares de la información.

X. CUMPLIMIENTO Y ACTUALIZACIÓN

El cumplimiento de esta política es obligatorio y su incumplimiento podrá generar sanciones conforme a la normativa interna y legal vigente. Esta política será revisada y actualizada de forma periódica, o cuando se presenten cambios normativos, tecnológicos o estratégicos que así lo requieran. Su divulgación y apropiación por parte de todos los actores institucionales es fundamental para consolidar una cultura organizacional orientada a la seguridad de la información y la protección de los datos personales.

RAFAEL HERNANDO MARTÍNEZ SALAZAR
C.C. No. 11.812.537
Representante Legal
NEW BIOLOGY S.A.S.
NIT. 900.464.195-3