**POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD**

¡Está Bien!, empresa de actividades de Call Center, establece que la información es fundamental para el desarrollo de sus actividades, motivo por el cual está comprometido a proteger los activos de información que contienen datos sensibles e información de: (clientes corporativos, usuarios, funcionarios, socios, proveedores, y todas las partes interesadas), orientando sus esfuerzos a la preservación de la confidencialidad, integridad, disponibilidad, a la continuidad de las operaciones, la administración y/o gestión de riesgos, la creación de cultura y conciencia de seguridad de la información y ciberseguridad en los funcionarios, contratistas, proveedores y personas que hagan uso de los activos de información de ¡Esta Bien! SAS, los controles establecidos en las políticas de seguridad descritas en el presente documento, están fundamentados según la ley 1581 de 2012.

Objetivos de la seguridad de la Información:

- Minimizar el riesgo en las funciones más importantes de la compañía.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de nuestros clientes, socios y empleados.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes de ¡ESTA BIEN! SAS
- Garantizar la continuidad del negocio frente a incidentes.

¡ESTA BIEN! SAS ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos y/o procesos claros acordes a las necesidades del negocio, y a los requerimientos regulatorios.

¡ESTA BIEN! SAS, define una Política de Ciberseguridad de la información orientada a gestionar eficazmente la seguridad de la información tratada por los sistemas informáticos, así como los activos críticos que participan en sus procesos, esta política tiene como objetivo garantizar la confidencialidad, integridad, disponibilidad y privacidad de la información ante posibles Ciberataques, y cumplir con las Leyes y Reglamentaciones.

Compromisos:

- Evaluar por anticipado los posibles riesgos en materia de Ciberseguridad.
- Procedimientos y responsabilidades de respuesta inmediata ante incidentes de ciberseguridad.
- Ofrecer un nivel apropiado de ciberseguridad durante el desarrollo de las actividades y operaciones.

- Garantizar que nuestros empleados son debidamente informados y capacitados en materia de ciberseguridad.
- Monitorización y detección de alertas tempranas que permitan una identificación permanente y continuada de las vulnerabilidades.