1. PRESENTACIÓN

INGERPROYECTOS protege, preserva y administra la integridad, confidencialidad, disponibilidad y autenticidad de la información, así como la seguridad digital y la gestión de la continuidad de la operación, conforme al mapa de procesos y en cumplimiento de los requisitos legales y reglamentarios, previniendo incidentes mediante la gestión de riesgos integrales en seguridad y privacidad de la información y seguridad digital, con la implementación de controles de seguridad físicos y digitales, orientados a la mejora continua en la gestión y el alto desempeño del Sistema de Gestión de Seguridad de la Información, con la finalidad de prestar servicios con calidad y transparencia de los procesos inherentes a nuestro objeto social.

2. ALCANCE

La política general aborda la necesidad de la implementación de un sistema de gestión de seguridad de la información (SGSI) planteado desde la descripción del ¿quién?, ¿qué?, ¿por qué?, ¿cuándo? y ¿cómo?, en torno al desarrollo de la implementación del SGSI. Es así como, teniendo en cuenta la importancia que tiene para INGERPROYECTOS cuenta con un alcance sus para sus colaboradores directos, aprendices, practicantes, proveedores, contratistas y clientes.

3. OBJETIVOS

Teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del SGSI estarán determinadas por las siguientes premisas:

- Mantener la confianza de sus clientes, socios y empleados.
- Proteger los activos tecnológicos.
- Fortalecer la cultura de seguridad de la información en nuestros colaboradores, terceros, aprendices, practicantes y clientes de **INGERPROYECTOS.**
- Garantizar la continuidad del negocio frente a incidentes.
- **INGERPROYECTOS** 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.

4. IMPLEMENTACIÓN

La gerencia de **INGERPROYECTOS**, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un sistema de gestión de seguridad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes colombianas y en concordancia con la misión y visión de la empresa. Para **INGERPROYECTOS** la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad,

confidencialidad y la disponibilidad de esta, acorde con las necesidades de los diferentes grupos de interés identificados.

La implementación de un sistema de seguridad debe estar complementado con las políticas de **INGERPROYECTOS**, y garantizando la integridad, confidencialidad y disponibilidad de la información. Los documentos relativos a las políticas de seguridad deben contemplar los procedimientos para hacer cumplir las reglas, las responsabilidades en todos los niveles. Todos ellos deben tener el apoyo gerencial de la organización.

Las políticas de seguridad deben ser conocidos por todo el personal de una organización, a través de este documento formal que reposará en las políticas de la organización y quedará en la carpeta pública para sensibilización con los colaboradores.

Entre los documentos pueden citarse los siguientes:

NAS carpeta de seguridad de la compañía, su contenido son subcarpetas por áreas y proyectos, donde la administración de usuarios que reglamentará el acceso a los recursos por el personal de la organización será suministrada únicamente por la Gerencia general de **INGERPROYECTOS**.

Copias de respaldo: Describirá los pasos a seguir para asegurar una adecuada recuperación de la información, a través de las copias de respaldo, realizadas por el área de tecnología en direccionamiento con la Gerencia general.

TRATAMIENTO DE LA INFORMACIÓN: Definirá claramente los tipos de información que es manejada por las personas autorizadas dentro de **INGERPROYETOS**.

SOFTWARE LEGAL: Definirá claramente el uso de software en la empresa con licencias de uso legal.

Uso del servicio de Internet y del correo electrónico: Describirá la protección de la información mediante el uso de correo electrónico y del servicio de Internet, de manera corporativa y con información.

AMBIENTES DE PROCESAMIENTO: Define el uso de los ambientes de procesamiento de información.

SEGURIDAD EN LAS COMUNICACIONES: Describirá la protección de la información durante los procesos de transmisión y recepción de datos en las redes internas y externas.

AUDITORÍAS DE LOS SISTEMAS: Que permitirá hacer un control de los eventos de seguridad de los sistemas.

CONTINUIDAD DEL PROCESAMIENTO: Se definirán y reglamentarán las actividades relativas a la recuperación de la información en casos críticos mediante una metodología adecuada.

PROTECCIÓN FÍSICA: Definirá la protección física de los equipos, de procesamiento, almacenamiento y transmisión de la información.

5. SANCIONES POR INCUMPLIMIENTOS

Este documento contemplará las medidas que se aplicarán por incumplimiento de las reglas definidas, En **INGERPROYECTOS** muchos trabajadores están constantemente manejando diferentes documentos de relativa importancia, los cuales deben tener un especial tratamiento y manejo para la consignación y garantizarían de la mejor gestión de los servicios que la entidad esté prestando. Algunas veces puede presentarse que estos documentos no son tratados de la manera que se espera y son modificados por los trabajadores sin ninguna autorización o sin los procedimientos que se esperan. En estas prácticas pueden existir delitos como la falsedad de documentos y otras prácticas que no solo son rechazados por **INGERPROYECTOS**, sino que son condenados de manera taxativa por parte del Estado.

El delito de falsedad de documento público es una conducta definida como dolosa y se encuentra tipificada por el artículo 287 del Código Penal, que establece:

“El delito de falsedad material en documento público se tipifica en caso de que el sujeto activo de la conducta punible sea una persona no cualificada como servidor público en ejercicio de funciones públicas, es decir debe ser un particular en sentido lato.

La acción típica es la de falsificar, que es la acción humana de contenido material que obra físicamente sobre el objeto documental para inculcar una calidad negativa, como la de ser falso.

Tal acción opera de dos maneras, modificando la prueba documental preexistente, o fabricando en su totalidad el objeto documental, en cuanto exista un desvalor de la acción de autor documental, en cuanto actué tendiendo a producir tal modificación un documento diverso y genuino.”

6. CONCLUSIÓN

La información es un recurso de suma importancia para la Empresa u organización y se la debe proteger a través de la implementación de las medidas de seguridad basadas en hardware, software y recursos humanos, pero también complementadas con adecuadas políticas de seguridad que sean conocidas por el personal de la organización en todos sus niveles. El personal de **INGERPROYECTOS** debe identificarse plenamente con los

objetivos de seguridad y protección que busca los objetivos mancomunados de nuestros colaboradores y la organización. La seguridad de la información es tarea de todos: del personal de la Empresa, de los Socios, de los accionistas, de los clientes.



Jorge Ernesto Sanchez Jalabe
Gerente General

7. APROBACIÓN

ELABORADO POR: Sandra Aranda **CARGO:** Director administrativo y comercial

REVISADO POR: Johana Arias **CARGO:** Coordinador SGI

APROBADO POR: Ing. Jorge Sanchez **CARGO:** Gerente

8. CONTROL DE CAMBIOS

VERSIÓN	DESCRIPCIÓN	FECHA	ELABORÓ	REVISÓ	APROBÓ
01	Generación del documento	22/01/2020	S. Aranda	S. Aranda	J. Sanchez
02	Revisión y actualización del documento Se modifica salud ocupacional por seguridad y salud en trabajo	26/06/2025	S. Aranda	J. Arias	J. Sanchez