POLITICA GENERAL SISTEMA DE GESTION SEGURIDAD DE LA INFORMACION

1. ACUERDO DE CONFIDENCIALIDAD

Este documento contiene información confidencial perteneciente a **ARQUITECSOFT S.A.S**, la misma constituye un secreto de industria, y está siendo entregada bajo el entendimiento de que será manejada en la más estricta confidencialidad; por lo tanto, no deberá ser revelada, duplicada o usada en su totalidad ni en parte de ella, para ningún propósito que no sea la evaluación de este material. De ninguna manera los asuntos descritos en este documento pueden ser revelados a otras personas, sólo a aquellas que sean aprobadas por los directivos de **ARQUITECSOFT S.A.S.**

2. OBJETIVO

Establecer la política general del sistema de gestión de seguridad de la información, responsabilidades, principios y directrices que deben de cumplir las partes interesadas frente al uso de los activos de información con el fin de regular la gestión de la seguridad de la información en la organización.

3. ALCANCE

La política contenida en este documento se establece, aplica y deberá ser conocida, aceptada y cumplida por todos los colaboradores, contratistas, practicantes, terceros, entre otros. El incumplimiento de esta se considerará un incidente de seguridad que, de acuerdo al caso, podrá dar lugar a un proceso disciplinario para los colaboradores o una causa válida para terminación de contratos establecidos con los terceros involucrados, sin perjuicio de la iniciación de otro tipo de acciones a las que haya lugar.

4. DEFINICIONES

Seguridad de la Información: se entiende como la preservación de las siguientes características:

Confidencialidad: Se garantiza que la información sea accesible solo a personas autorizadas.

Integridad: Cuando la información es exacta y completa.

Disponibilidad: Cuando la información es accesible a los usuarios autorizados.

Autenticidad: Cuando se garantiza la identidad de quien solicita acceso a la información.

No repudio: Es la forma de evitar que quien envió o recibió información alegue que no lo realizó ante terceros.

Legalidad: Referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeta la Compañía.

Confiabilidad: La información generada es la adecuada para la toma de decisiones.

5. DECLARACION

En **ARQUITECSOFT S.A.S.**, conocemos la importancia y el valor de la información tanto interna como de nuestros clientes, por eso se compromete adoptar las mejores prácticas de seguridad de la información, buscando proteger la confidencialidad, integridad, disponibilidad y confiabilidad de la información en sus procesos y servicios, como en el cumplimiento de los requerimientos de los diferentes grupos de interés, incluyendo los legales, reglamentarios y los aplicables; promoviendo una cultura de seguridad y compromiso con la mejora continua.

5.1. OBJETIVOS DE SEGURIDAD DE LA INFORMACION

Para dar cumplimiento a esta política general, se establecen los siguientes objetivos:

1. Gestionar el riesgo de seguridad de la información en las actividades más importantes y críticas implementando medidas de tratamiento con controles.
2. Apoyar la innovación tecnológica, buscando la mejora continua en todos nuestros servicios y productos.
3. Identificar y Proteger los activos de la información, gestionando los incidentes que puedan provocar la perdida de Confidencialidad, Integridad y Disponibilidad.
4. Fortalecer la cultura de seguridad de la información en los colaboradores, contratistas y clientes de ARQUITECSOFT S.A.S.
5. Identificar todas las regulaciones y normativas vigentes a dar cumplimiento internamente como por nuestros clientes.

Para el desarrollo de la estrategia se implementará una cultura organizacional enfocada en identificar y evaluar los riesgos de acuerdo con los objetivos de la compañía tomando como base los criterios de clasificación, evaluación y valoración, descritos en la metodología de riesgo para la definición de controles relacionados con la seguridad y la búsqueda hacia la mejora continua, teniendo en cuenta los requerimientos de nuestras partes interesadas para incrementar la credibilidad y la confianza de los procesos y garantizar la confidencialidad, integridad y disponibilidad de la información y de los activos tecnológicos.

6. COMPROMISO

La Alta Dirección de ARQUITECSOFT S.A.S., aprueba esta Política de Seguridad de la información como muestra de su compromiso y apoyo en el diseño e implementación de políticas eficientes que garanticen la seguridad de la información de la Compañía. La Alta Dirección de la Entidad demuestran su compromiso a través de:

La revisión y aprobación de las Políticas de Seguridad de la información.

La promoción activa de una cultura de seguridad.

La promoción y divulgación de las políticas a todos los colaboradores de la compañía.

El aseguramiento de los recursos adecuados para implementar y mantener las políticas de seguridad de la información.

La política general y específicas de la seguridad de la información serán revisada anualmente como parte del proceso de mejora continua, o cuando se identifiquen cambios en su estructura, sus objetivos o alguna condición que afecten a la misma, para asegurar que sigue siendo adecuada, conveniente y eficaz, ajustada a los requerimientos identificados.

7. RESPONSABILIDADES

ARQUITECSOFT S.A.S., establece una estructura organizacional responsable de la seguridad de la información, con roles y responsabilidades claramente definidos, teniendo en cuenta actividades para la gestión de riesgos, análisis de las tecnologías y del entorno, promueve la cultura de la seguridad e informa del desempeño del Sistema de Gestión de Seguridad de la Información a la Alta Dirección.

La Alta Dirección es responsable de la aprobación de la Política de Seguridad de la Información, con el fin de garantizar la seguridad de la información y la continuidad de la operación de la compañía.

El Oficial de Seguridad de la Información es el encargado de la revisión y difusión de las Políticas de Seguridad de la Información.

El Comité de Seguridad de la Información es el responsable de tratar los incidentes de seguridad que se presenten y tomar las decisiones apropiadas que permitan mantener correctamente el sistema de gestión de seguridad de la información en la compañía.

Los propietarios de activos de información son responsables del uso adecuado y de la preservación del correcto estado de los mismos.

El Proceso de Talento Humano es responsable por determinar y ejecutar las sanciones que se deriven del incumplimiento de las políticas de Seguridad de la Información por parte del personal de la compañía.

Todos los colaboradores, contratistas, practicantes y terceros son responsables y deben comprometerse a cumplir con todas las Políticas de Seguridad de la Información.

8. SANCIONES POR INCUMPLIMIENTO

El incumplimiento de las Políticas de Seguridad de la Información se gestiona mediante procedimientos administrativos, cuando se identifique un incumplimiento a la presente Política se deberá reportar al Oficial de Seguridad de la Información de la compañía utilizando los canales definidos para dicho fin, para los efectos de su competencia y atribuciones. Se consideran violaciones graves el robo, daño, divulgación de información reservada o confidencial de la compañía o los delitos informáticos contemplados en el artículo 269 de la ley 1273 de 2009.

9. CONTROL DE CAMBIOS

Versión	Fecha	Descripción del Cambio	Elaborado por	Revisado por	Aprobado por
1.0	2023-06-13	Creación de la política general del sistema de gestión de seguridad de la información	Christian Marín / SIG	Comité Mejora Continua	Rubén Darío Díaz / Líder de Gestión de Mejora Continua
2.0	2023-11-24	Cambio de logo	Juan Pablo Navarro / Coordinador Gestión de Mejora continua	José Alfredo Montaño / Líder Gestión de Mejora Continua	José Alfredo Montaño / Líder Gestión de Mejora Continua
3.0	2025-09-24	Se revisa la política general de seguridad.	Juan Pablo Navarro / Coordinador Gestión de Mejora continua	José Alfredo Montaño / Líder Gestión de Mejora Continua	José Alfredo Montaño / Líder Gestión de Mejora Continua