# Política de seguridad de la información

## Tabla de Contenido


1. Marco Contextual ..... 2
1.1 Objetivo ..... 2
1.2 Alcance ..... 2
1.3 Responsable ..... 3
1.4 Glosario ..... 3
2 Contenido ..... 4
2.1 Objetivos del Sistema de Gestión de Seguridad de la información ..... 4
2.2 Responsabilidades y cultura de seguridad de la información ..... 4
2.3 Política de alto nivel del SGSI ..... 5
2.4 Principios para la seguridad de la información: ..... 6
2.5 Directrices generales de seguridad de la información ..... 7
2.6 Gestión de excepciones ..... 8
2.7 Compromiso con el mejoramiento continuo ..... 9
2.8 Modelo de consecuencias ..... 9
3 Documentos Anexos ..... 10
4 Control de cambios ..... 10


# 1. Marco Contextual

## 1.1 Objetivo

Establecer lineamientos generales, principios y responsabilidades para preservar la confidencialidad, integridad y disponibilidad de la información de ARQUIB GROUP, con el fin de salvaguardar y proteger los activos de información que procesan, almacenan o transfieren información frente a amenazas internas y externas, asegurando una adecuada gestión de los riesgos de seguridad de la información y la alineación con los objetivos estratégicos.

## 1.2 Alcance

Esta política aplica a todas las empresas del GRUPO INVERSIONES ARQUIB S A S (En adelante ARQUIB GROUP), así como a los colaboradores, contratistas, consultores, personal

temporal, proveedores, terceros y demás partes interesadas que tengan acceso a información de ARQUIB GROUP o bajo su custodia.

### 1.3 Responsable

- Gerencia de IT
- Area de Seguridad de la información
- Todos los colaboradores

### 1.4 Glosario

- **SEGURIDAD DE LA INFORMACIÓN:** Preservación de la confidencialidad, integridad y disponibilidad de la información mediante la implementación de controles tecnológicos, organizacionales, físicos y de personas.
- **ACTIVOS DE INFORMACIÓN:** Cualquier información, sistema o recurso que crea, procesa, almacena o transmite datos y que es crítico para la organización, por lo que debe protegerse frente a riesgos que afecten su confidencialidad, integridad y disponibilidad.
- **DISPONIBILIDAD:** Garantía de que la información y los sistemas estarán accesibles en el momento que se requieran.
- **INTEGRIDAD:** Garantía de que la información se mantiene exacta, completa y sin alteraciones indebidas.
- **CONFIDENCIALIDAD:** Propiedad de la información de no estar disponible ni ser revelada a personas, entidades o procesos no autorizados
- **INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN:** Evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.
- **RIESGO DE SEGURIDAD DE LA INFORMACIÓN:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.
- **CONTROLES DE SEGURIDAD:** Medidas, prácticas, procedimientos o mecanismos implementados para reducir, gestionar o mitigar riesgos de seguridad de la información.

- **SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI):** Conjunto de políticas, procesos, procedimientos y controles que permiten gestionar de manera sistemática la seguridad de la información dentro de una organización.

## 2 Contenido

### 2.1 Objetivos del Sistema de Gestión de Seguridad de la información

- Salvaguardar y proteger los activos de información de Grupo Arquib, garantizando los principios de confidencialidad, integridad y disponibilidad de la información, conforme al marco normativo interno establecido.
- Gestionar los riesgos de seguridad de la información de ARQUIB GROUP para garantizar el cumplimiento del apetito del riesgo corporativo.
- Establecer controles de seguridad orientados a garantizar la confidencialidad, integridad y disponibilidad de los activos de información críticos que soportan la prestación de los servicios del Grupo Arquib, con el fin de prevenir incidentes y proteger los intereses de la organización.
- Fortalecer la cultura organizacional en seguridad de la información mediante la implementación de programas de concientización y capacitación, dirigidos a colaboradores y terceros.

### 2.2 Responsabilidades y cultura de seguridad de la información

- Todos los colaboradores, terceros, proveedores, contratistas y demás partes interesadas serán responsables de proteger la información a la cual tengan acceso, así como de cumplir los lineamientos establecidos en el sistema de Gestión de Seguridad de la información.
- Los roles y responsabilidades especificas se encuentran definidas y documentados en el documento DESCRIPTOR DEL CARGO, lineamientos internos vigentes y demás documentos aplicables.
- Los colaboradores y terceros deben dar cumplimiento a las directrices de seguridad de la información establecidas en las políticas, manuales, procedimientos y demás documentos del sistema de gestión de seguridad de la información definidos por la organización.

- La organización debe promover la cultura de seguridad de la información por medio de programas permanentes de capacitación, concientización con el fin de promover buenas prácticas de seguridad de la información y asegurar el cumplimiento de los lineamientos establecidos.
- Cualquier colaborador o tercero que incurra en el cumplimiento de las políticas del gobierno de seguridad de la información asumirá las medidas disciplinarias, contractuales, administrativas o legales conforme a la normatividad vigente
- Todos los gerentes deben velar por el cumplimiento de los lineamientos de seguridad de la información y darlas a conocer al interior de su equipo de trabajo

### 2.3 Política de alto nivel del SGSI

ARQUIB GROUP reconoce la importancia de proteger la confidencialidad, integridad y disponibilidad de la información perteneciente a la entidad, así como los activos de información y el cumplimiento de los requisitos legales y regulatorios aplicables. Con el propósito de salvaguardar la información, la Alta Dirección establece la implementación de un Sistema de Gestión de seguridad de la información alineado con los objetivos estratégicos aplicables, garantizando que los controles de seguridad implementados sean consistentes con las obligaciones regulatorias y necesidades del negocio.

La gestión de seguridad de la información se fundamenta en un enfoque basado en riesgos, que contempla la identificación, análisis y evaluación de riesgos de seguridad de la información que pueda afectar los activos de información. Este enfoque se complementa con la implementación de controles orientados a la mitigación de riesgos, contribuyendo a garantizar la protección de la información perteneciente a Grupo Arquib.

La alta Dirección reconoce la seguridad de la información como un componente estratégico para generar confianza en los clientes y demás partes interesadas, asumiendo un papel fundamental de liderar, respaldar y suministrar los recursos necesarios para promover la mejora y cumplimiento de los objetivos del sistema de gestión de seguridad de la información-alineados con la dirección estratégica de la organización.

De igual forma, la Alta Dirección promueve la cultura organizacional orientada a la seguridad de la información, apoyando la integración de los requisitos del sistema de gestión de seguridad de la información en los procesos de la organización y asegurando la adecuada asignación de roles y responsabilidades necesarios para la operación eficaz. Esto traduce en un compromiso firme con la seguridad de la información, el cumplimiento de los requisitos y refleja la determinación de fomentar prácticas de seguridad reconocidas.

Esta política demuestra el compromiso de ARQUIB GROUP con la excelencia e integridad en la gestión de la información, promoviendo un entorno seguro basado en los principios de confidencialidad, integridad y disponibilidad de la información. De esta forma, se salvaguarda los intereses de los clientes, colaboradores y demás partes interesadas de ARQUIB GROUP, fortaleciendo la confianza y el cumplimiento de los lineamientos organizacionales.

Esta política, junto con sus respectivos objetivos, los cuales son medibles y coherentes con el contexto organizacional, serán sometidos a revisiones periódicas al menos una vez al año, o cuando se presenten cambios relevantes en el contexto del negocio o normatividad aplicable según corresponda.

**2.4 Principios para la seguridad de la información:**

ARQUIB GROUP garantizará los siguientes principios:

- **Integridad:** La información debe ser completa, precisa y protegida contra modificaciones no autorizadas.
- **Confidencialidad:** La información debe ser accesible únicamente por personas autorizadas y no será divulgada sin previa autorización, manteniéndola en secreto y protegida contra el acceso no autorizado.
- **Disponibilidad:** La información debe estar disponible cuando sea requerida para la operación del negocio.

## 2.5 Directrices generales de seguridad de la información

ARQUIB GROUP establece su compromiso en la implementación de controles orientados a mitigar riesgos asociados a accesos no autorizados, con el fin de proteger los activos de información. Estos controles incluyen el uso de contraseñas robustas, la aplicación del principio de mínimo privilegio y la gestión de accesos a través de matriz de roles y perfiles, en alineación con las mejores prácticas de seguridad establecidas para el cumplimiento, garantizando que únicamente las personas autorizadas accedas a los activos de información conforme a sus responsabilidades laborales, así como la implementación de mecanismo de autenticación segura para prevenir accesos no autorizados.

Respecto a los entornos tecnológicos, se implementa controles de seguridad en la nube con el propósito de proteger los servicios, plataformas e infraestructura, garantizando configuraciones seguras, monitoreo continuo, segregación de ambientes y la adopción de buenas prácticas. De igual manera, se emplean mecanismos criptográficos para proteger la confidencialidad, integridad y autenticidad de la información sensible, estableciendo controles para la adecuada gestión del ciclo de vida de las claves criptográficas.

En cuanto a la gestión de vulnerabilidades, se establece un proceso continuo de identificación, evaluación, priorización, remediación y monitoreo de vulnerabilidades que puedan afectar los activos de información.

Frente a eventos de seguridad, se implementan mecanismos para la detección, reporte, análisis, contención, respuesta, recuperación, documentación y base del conocimiento de los eventos o incidentes, asegurando una comunicación oportuna que permite minimizar el impacto en la operación.

Adicionalmente, se adoptan prácticas de seguridad durante todo el ciclo de vida del desarrollo de software, integrando principios de DevSecOps, validaciones de seguridad y pruebas técnicas para reducir riesgos de seguridad de la información.

En materia de infraestructura, se establecen controles de seguridad para redes, restringiendo el acceso exclusivamente a personal autorizado, con el fin de proteger la información y los sistemas, entre otras aplicaciones de controles enfocados a la minimización del riesgo.

Así mismo se aplican controles de seguridad sobre los dispositivos y equipos corporativos, tales como el cifrado por medio de herramientas robustas, con el fin de proteger la información y salvaguardar la confidencialidad, integridad y disponibilidad de la información. De igual forma, se establecen configuraciones seguras, limitando privilegios de acceso y restringiendo modificaciones en los equipos por parte de personal no autorizado, reduciendo riesgos relacionados a acceso no autorizados, perdida de la información, entre otros

ARQUIB GROUP dentro de sus controles de seguridad realiza respaldos a la información, que contemplan mecanismos de retención, recuperación, entre otros, garantizando su disponibilidad y recuperación oportuna ante fallas, incidentes o desastres.

Todo proveedor que mantengan una relación contractual con ARQUIB GROUP deberá cumplir con los requisitos de seguridad de la información acordes a la evaluación de los riesgos de seguridad de la información asociados al servicio prestado, incorporando cláusulas de seguridad de la información con los proveedores como garantía de cumplimiento

ARQUIB GROUP cuenta con políticas especificas de seguridad de la información donde se definen los principales controles del sistema de gestión de seguridad de la información.

**2.6 Gestión de excepciones**

Cualquier excepción a lo establecido en la política de seguridad de la información deberá ser documentada formalmente, con su respectivo análisis y aceptación de riesgos. Así mismo, deberá contar con la aprobación de las áreas responsables, un periodo de vigencia definido y un esquema de revisiones periódicas.

Ninguna excepción podrá implementarse sin la autorización formal y debe tener controles compensatorios que mitiguen los riesgos asociados.

## 2.7 Compromiso con el mejoramiento continuo

Bajo el liderazgo de la Alta Dirección, la organización manifiesta su firme compromiso con la mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI). En este sentido, se llevarán a cabo evaluaciones periódicas del desempeño en materia de seguridad de la información, así como de la efectividad de los controles implementados, con el propósito de asegurar que la presente política y sus lineamientos asociados se mantengan actualizados y evolucionen conforme a los cambios en el entorno tecnológico, las amenazas emergentes, los resultados de auditorías y los requisitos legales y contractuales aplicables.

De igual manera, todos los colaboradores, contratistas y terceros están obligados a participar de manera activa y responsable en este proceso de mejora continua, informando oportunamente cualquier debilidad, incidente o incumplimiento al área de Seguridad de la Información. Lo anterior, con el fin de garantizar un entorno de información resiliente, seguro y plenamente alineado con las necesidades estratégicas de la organización.

## 2.8 Modelo de consecuencias

Todas las empresas del Grupo Arquib, así como a los colaboradores, contratistas, consultores, personal temporal, proveedores, terceros y demás partes interesadas tienen la responsabilidad de cumplir esta Política de seguridad de la información. Cualquier incumplimiento de esta política, puede constituir una falta y se aplicarán las medidas disciplinarias correspondientes de manera proporcional según su gravedad, intencionalidad y reincidencia.

## 3 Documentos Anexos

## 4 Control de cambios

| VERSIÓN | FECHA | CAMBIO REALIZADO | MOTIVO DEL CAMBIO |
|---|---|---|---|
| 1 | 18/05/2026 | Creación de política | Nueva política |