



POLÍTICA GENERAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

1.1 Generalidades

Esta política se aplica a todo el Sistema de Gestión de Seguridad de la Información – SGSI.

El propósito de esta política de alto nivel es definir el objetivo, dirección, principios y reglas básicas para la gestión de la seguridad de la información y ciberseguridad, y aplica a todas las partes interesadas internas y externas que accedan física y/o remotamente a los activos de información y ciber activos propiedad de Banco Finandina.

1.2 Política

El Banco Finandina reconoce la imperante necesidad de salvaguardar la confidencialidad, integridad y disponibilidad de la información de la entidad, así como proteger los activos de información críticos, al tiempo que busca cumplir con los requisitos legales y regulatorios aplicables. Con el firme compromiso de fortalecer nuestra postura en seguridad, la Alta Dirección del Banco ha decidido implementar un Sistema de Gestión de Seguridad de la Información – SGSI de acuerdo con los lineamientos del estándar ISO27001:2022.

El enfoque integral hacia la seguridad de la información se basa en la identificación, evaluación y gestión proactiva de los riesgos asociados. El Banco Finandina se compromete a mejorar continuamente el Sistema de Gestión de Seguridad de la Información – SGSI en respuesta a los cambios tecnológicos, las amenazas emergentes y los requisitos dinámicos del negocio.

Esta política de seguridad de la información refleja nuestro compromiso inquebrantable con la excelencia y la integridad en la gestión de la información.

1.3 Objetivos del SGSI

Los objetivos generales para el Sistema de Gestión de Seguridad de la Información – SGSI son los siguientes:

- a) Preservar la confidencialidad, integridad y disponibilidad de la información, de acuerdo con las políticas, procedimientos y demás documentación para la gestión en el Banco Finandina.
- b) Gestionar los riesgos de seguridad de la información y ciberseguridad para garantizar el cumplimiento del apetito de riesgo corporativo.
- c) Establecer controles técnicos, administrativos y de vigilancia, con el fin de proteger la confidencialidad, integridad y disponibilidad de los activos de información y ciber activos críticos para la operación y servicios prestados por el banco.



Banco Finandina
Banca libre

- d) Establecer una cultura y comportamiento de cumplimiento y protección de la seguridad de la información y ciberseguridad para todo el personal del Banco Finandina, aliados, contratistas y terceros vinculados con la prestación de los servicios.
- e) Cumplimiento de requisitos legales, reglamentarios asociados a seguridad de la información y ciberseguridad.
- f) Brindar las herramientas necesarias para el desarrollo, maduración y mejoramiento continuo del Sistema de Gestión de Seguridad de la Información – SGSI
- g) Fortalecer la cultura de seguridad de la información en colaboradores, proveedores, clientes y demás partes interesadas de nuestros servicios.

La presente política es de aplicación obligatoria para todos los empleados, aliados, contratistas y terceros que manejen información del banco.