# POLÍTICA DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

CAMARA DE COMERCIO
DE MEDELLIN PARA ANTIOQUIA

## 1. OBJETIVO

Establecer los objetivos, principios, compromisos y responsabilidades para la gestión de la seguridad de la información en la Cámara de Comercio de Medellín para Antioquia, garantizando la protección de los activos de información y tecnológicos mediante la preservación de la confidencialidad, integridad y disponibilidad de la información, la gestión de los riesgos asociados y el fortalecimiento de una cultura organizacional orientada a su uso seguro y responsable, contribuyendo al cumplimiento de los objetivos estratégicos, la generación de valor para los grupos de interés, el cumplimiento de los requisitos aplicables y la continuidad operativa de la organización

## 2. ALCANCE

La presente Política del Sistema de Gestión de Seguridad de la Información aplica a todos los procesos, servicios, activos de información, activos tecnológicos, colaboradores, contratistas, proveedores y terceros que, en el desarrollo de sus funciones o de la prestación de servicios para la Cámara de Comercio de Medellín para Antioquia, creen, accedan, procesen, almacenen, transmitan o administren información de propiedad o bajo responsabilidad de la organización.

Esta política es de aplicación en todas las sedes, canales de atención, ambientes tecnológicos y servicios administrados por la organización o por terceros en su nombre.

Las iniciativas relacionadas con la Gestión de Información, Gobierno de Información y demás capacidades organizacionales asociadas serán desarrolladas mediante los procesos, modelos de gobierno, lineamientos y procedimientos específicos que se definan e implementen posteriormente.

## 3. MARCO NORMATIVO

ISO 27001 Sistema de Gestión de Seguridad de la Información.

## 4. DESARROLLO DE LA POLÍTICA

En la Cámara de Comercio de Medellín para Antioquia trabajamos para que las empresas e instituciones cívicas, sociales y culturales de la región crezcan, siendo un aliado en su desarrollo. Por esta razón implementamos los procesos, prácticas, controles y estructuras requeridos para cumplir nuestras funciones delegadas y demás iniciativas de desarrollo empresarial, garantizando altos estándares de seguridad, protección y gestión de la información. La información es reconocida como un activo estratégico para el cumplimiento

de nuestro propósito institucional, la generación de valor para nuestros grupos de interés y la toma de decisiones basada en datos confiables.

La Cámara de Comercio de Medellín para Antioquia establece el Sistema de Gestión de Seguridad de la Información (SGSI) como un mecanismo para proteger los activos de información, gestionar los riesgos asociados y fortalecer una cultura organizacional orientada al uso responsable y seguro de la información.

## Objetivos del Sistema de Gestión de Seguridad de la Información

El SGSI tiene como objetivos:

- Diseñar, implementar y mantener los procesos, controles y herramientas tecnológicas que garanticen la disponibilidad, integridad y confidencialidad de la información, así como la continuidad operativa de la organización.
- Minimizar la ocurrencia y recurrencia de incidentes y eventos que puedan afectar la seguridad de la información y la operación institucional.
- Promover el desarrollo de una cultura organizacional orientada al manejo seguro y responsable de la información.
- Fortalecer las capacidades organizacionales para la gestión, protección y aprovechamiento seguro de la información como activo estratégico para la generación de valor y la toma de decisiones.

## Compromisos de la Organización

Para el cumplimiento de estos objetivos, la Cámara de Comercio de Medellín para Antioquia se compromete a:

- Prestar servicios de calidad, pertinentes y oportunos, soportados en tecnología y en prácticas de gestión de la información que permitan garantizar la seguridad, confiabilidad y disponibilidad de la información requerida por nuestros grupos de interés.
- Disponer y administrar los recursos necesarios para alcanzar una cobertura integral de los aspectos relativos a la seguridad de la información, la ciberseguridad y la continuidad del negocio.
- Establecer los criterios para la recolección, creación, captura, almacenamiento, procesamiento, uso, intercambio, conservación y disposición final de la información y de los datos personales tratados por la organización, garantizando el cumplimiento de la normatividad aplicable y los derechos de los titulares.
- Gestionar los riesgos asociados a los activos de información y a los activos tecnológicos, aplicaciones y mecanismos mediante los cuales la información es creada, procesada, almacenada o compartida.

- Promover la disponibilidad de información confiable, íntegra y oportuna para apoyar la toma de decisiones, la prestación de servicios y el cumplimiento de los objetivos estratégicos de la organización.
- Definir e implementar planes de contingencia, recuperación y respuesta ante incidentes y emergencias que permitan proteger y recuperar la información requerida para asegurar la continuidad del negocio.
- Mantener procesos continuos de verificación, evaluación y pruebas de funcionamiento de los controles, políticas y lineamientos asociados a la seguridad de la información.
- Cumplir los requisitos legales, regulatorios, contractuales y organizacionales aplicables, promoviendo la mejora continua del Sistema de Gestión de Seguridad de la Información.

### Declaración de Mejora Continua

La Cámara de Comercio de Medellín para Antioquia mantendrá un enfoque permanente de mejora continua sobre su Sistema de Gestión de Seguridad de la Información, fortaleciendo progresivamente sus capacidades para proteger, gestionar y aprovechar la información de manera segura, confiable y alineada con su direccionamiento estratégico, las necesidades de sus grupos de interés y la evolución de los riesgos del entorno.

## 5. ROLES Y RESPONSABILIDADES

**Alta Dirección**

Es responsable de:

- Aprobar la presente política y realizar seguimiento al desempeño del Sistema de Gestión de Seguridad de la Información en intervalos planificados.
- Proporcionar los recursos necesarios para establecer, implementar, operar, monitorear, mantener y mejorar continuamente el sistema de gestión.
- Promover una cultura organizacional orientada a la protección y gestión responsable de la información.

**Líder del SGSI (Director de Tecnología)**

Es responsable de:

- Definir los procesos, lineamientos, directrices y documentos de apoyo relacionados con la seguridad de la información, de acuerdo con los estándares normativos y la legislación aplicable.
- Identificar, evaluar, tratar y monitorear los riesgos asociados a la seguridad de la información.
- Monitorear el desempeño del Sistema de Gestión de Seguridad de la Información.

- Identificar e implementar acciones de mejora continua del sistema.
- Coordinar y atender los procesos de auditoría relacionados con el SGSI.
- Promover la articulación entre la seguridad de la información y las iniciativas organizacionales de gestión de información, gobierno de datos y transformación digital.

**Colaboradores y Usuarios de la CCMA**

Son responsables de:

- Cumplir las políticas, lineamientos y controles definidos para garantizar la integridad, disponibilidad y confidencialidad de la información.
- Reportar oportunamente eventos, incidentes o situaciones de riesgo relacionadas con la seguridad de la información.
- Informar sobre debilidades observadas o sospechadas en sistemas, servicios o controles de seguridad.
- Utilizar adecuadamente la información y las bases de datos bajo su responsabilidad, respetando la normatividad vigente y los derechos de los titulares de los datos.
- Participar en las actividades de sensibilización y capacitación relacionadas con seguridad de la información, protección de datos y uso responsable de la información.

**Proveedores y Terceros**

Son responsables de:

- Cumplir las políticas, lineamientos y requisitos de seguridad definidos por la organización y aquellos establecidos contractualmente.
- Garantizar la confidencialidad, integridad y disponibilidad de la información bajo su responsabilidad durante la prestación de servicios.
- Reportar oportunamente incidentes, eventos o vulnerabilidades relacionadas con la seguridad de la información.
- Participar en los procesos de sensibilización y cumplimiento que la organización determine cuando aplique.

Daniel Osorio
**Daniel Fernando Osorio Giraldo**
**Vicepresidente Administrativo y Desarrollo Organizacional**

# Certificado de firma

Para los efectos legales pertinentes, **la parte manifiesta que ha decidido suscribir el presente documento de manera electrónica** , y declara que la firma estampada en el mismo ha sido puesta por quien dice ser su firmante cumpliendo todos los requisitos legales para este tipo de firmas, y por ello,**reconoce la plena validez tanto de lo dispuesto en el clausulado del presente documento** como de la firma electrónica que en él se asientan.

## Autenticidad

DFOG

Daniel Fernando Osorio Giraldo
Autenticado con:
Correo electrónico
Teléfono
Código OTP

**Hash de firmante:**
f22c436184ec1b9ec06af73bd87f8be92961afea81366ce14080a2f9f9e22b59

| | |
|---|---|
| E-mail | dani**********com.co |
| Teléfono | +57******5702 |
| IP | 201.232.238.151 |
| Rol | Firmante |
| Firmado | 11/9/26, 17:08:07 GMT-5 |

## Integridad del documento

Número de documento: Q06KZH9U19

Función Hash: SHA-256

Hash del documento: df796f876b76609729b03ee9ce5655818059c431b059f594c102351192be983a

## Disponibilidad del documento

El documento puede ser consultado a través de su número de identificación y/o código QR en nuestra plataforma **www.auco.ai/verify**