**D-TIC-024**

# POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

**V.02 del 12 de octubre 2023 R.04 del 12 de octubre 2023**

## 1. INTRODUCCIÓN

La información es un activo importante para la organización, el cuál debe ser protegido adecuadamente. Con el avance tecnológico y la creciente interconexión, este activo se ve cada vez más amenazado, e independientemente de su forma, impresa o escrita en un papel, almacenada electrónicamente, transmitida por correo o utilizando medios electrónicos, se expone a una gran variedad de amenazas y vulnerabilidades.

Con el fin de garantizar la continuidad de los sistemas de información, minimizar los riesgos de daños y asegurar el eficiente cumplimiento de los objetivos de la organización, se implementan controles que gestionen la seguridad de la información, los cuales incluyen políticas, procesos, procedimientos, estructuras organizacionales y funciones de software y hardware.

Se necesita establecer, implementar, monitorear, revisar y mejorar estos controles cuando sea necesario, para asegurar que se cumplan los objetivos de seguridad y comerciales específicos.

## 2. OBJETIVOS

- Proteger los recursos de información del CENTRO COMERCIAL SANTAFÉ MEDELLÍN P.H. y la tecnología utilizada para su procesamiento, frente a amenazas internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.
- Proporcionar a la gerencia el direccionamiento y soporte, para la seguridad de la información, en concordancia con los requerimientos comerciales y las leyes y regulaciones relevantes.
- Mantener la Política de Seguridad actualizada, con el fin de asegurar su vigencia y nivel de eficacia.

## 3. ALCANCE

Esta Política se aplica al CENTRO COMERCIAL SANTAFÉ MEDELLIN P.H., a sus recursos y a la totalidad de los procesos, ya sean internos o externos, vinculados a la entidad a través de contratos o acuerdos con terceros.

## 4. RESPONSABILIDADES

Todos los directivos del CENTRO COMERCIAL SANTAFÉ MEDELLÍN P.H., son responsables de la implementación de esta política de seguridad de la información, dentro de sus áreas de gestión, así como del cumplimiento de dicha política por parte de su equipo de trabajo.

La Política de Seguridad de la Información, es de aplicación obligatoria para todo el personal de la organización, de todas las áreas y sea cualquiera que sea el nivel de tareas que desempeñe.

Es responsabilidad de La **Gerencia General** aprobar esta Política y la autorización de sus modificaciones.

La **Coordinación de Tecnología** procederá a revisar y proponer a la Gerencia General del Centro Comercial Santafé Medellín P.H., la aprobación de la Política de Seguridad de la Información, y las funciones generales en materia de seguridad de la información; monitorear cambios significativos en los riesgos que afectan los recursos de información frente a las amenazas más importantes; tomar conocimiento y supervisar la investigación y monitoreo de los incidentes relativos a la seguridad; aprobar las principales iniciativas para incrementar la seguridad de la información, de acuerdo a las competencias y responsabilidades asignadas a cada área, así como acordar y aprobar metodologías y procesos específicos relativos a seguridad de la información; garantizar que la seguridad sea parte del proceso de planificación de la información, evaluar y coordinar la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios; promover la difusión y apoyo a la seguridad de la información dentro de la organización y coordinar el proceso de administración de la continuidad de las actividades de la organización.
El **Analista de Tecnología y Auxiliar de Sistemas** cumplirán funciones relativas a la seguridad de los sistemas de información de la organización, incluyendo la supervisión e implementación de todos los aspectos tratados en la presente Política. Deberán implementar y supervisar el cumplimiento de las políticas, procedimientos y prácticas definidas en el marco de ésta política.

Los **Propietarios de la Información** (desde el punto de vista técnico no jurídico)**,** son responsables de clasificarla de acuerdo con el grado de sensibilidad y criticidad de la misma, de

documentar y mantener actualizada la clasificación efectuada y de definir qué usuarios deberán tener permisos de acceso a la información de acuerdo a sus funciones y competencia.

El **Responsable de Desarrollo Humano**, cumplirá la función de notificar a todo el personal que ingresa, de sus obligaciones respecto del cumplimiento de la Política de Seguridad de la Información y de todas las normas, procedimientos y prácticas que de ella surjan. Así mismo, tendrá a su cargo la notificación de la presente Política a todo el personal, así como de los cambios que en ella se produzcan, la implementación de la suscripción de los compromisos de Confidencialidad y las tareas de capacitación continua en materia de seguridad.

El **Responsable del Área Legal** verificará el cumplimiento de la presente Política en la gestión de todos los contratos, acuerdos u otra documentación de la organización con sus empleados y con terceros. Así mismo, asesorará en materia legal a la organización, en lo que se refiere a la seguridad de la información.

Los **usuarios de la información y de los sistemas** utilizados para su procesamiento, son responsables de conocer, dar a conocer, cumplir y hacer cumplir la Política de la Seguridad de la Información vigente.

El responsable de la **Auditoría Interna** o quién sea propuesto por el equipo de Seguridad de la Información, es responsable de practicar auditorías periódicas sobre los sistemas y actividades vinculadas con la tecnología de información, debiendo informar sobre el cumplimiento de las especificaciones y medidas de seguridad de la información establecidas por esta Política y por las normas, procedimientos y prácticas que de ella surjan.

## 5. ASPECTOS GENERALES

Esta Política se conforma de una serie de pautas sobre aspectos específicos de la Seguridad de la Información, que incluyen los siguientes tópicos:

- Los activos de información del CENTRO COMERCIAL SANTAFÉ MEDELLÍN P.H., serán identificados y clasificados para establecer los mecanismos de protección necesarios.

- El CENTRO COMERCIAL SANTAFÉ MEDELLÍN P.H., definirá e implantará controles para proteger la información contra violaciones de autenticidad, accesos no autorizados, la pérdida de integridad y que garanticen la disponibilidad requerida por los clientes y usuarios de los servicios ofrecidos por la organización.
- Todos los funcionarios y/o contratistas, serán responsables de proteger la información a la cual accedan y procesen, para evitar su pérdida, alteración, destrucción o uso indebido.
- Únicamente se permitirá el uso de software autorizado que haya sido adquirido legalmente por la organización.
- Es responsabilidad de todos los funcionarios y contratistas del Centro Comercial Santafé Medellín, reportar los incidentes de Seguridad, eventos sospechosos y el mal uso de los recursos que identifique.
- Las violaciones a las Políticas y Controles de Seguridad de la información serán reportadas y se tratarán según las disposiciones contractuales y legales.
- El CENTRO COMERCIAL SANTAFÉ MEDELLÍN P.H. contará con un Plan de Continuidad del Negocio, que asegure la continuidad de las operaciones, ante la ocurrencia de eventos no previstos o desastres naturales.
- El CENTRO COMERCIAL SANTAFÉ MEDELLÍN P.H. implantará todos los controles destinados a impedir infracciones y violaciones de las leyes del derecho civil y penal de las obligaciones establecidas por las leyes, estatutos, normas, reglamentos o contratos; y de los requisitos de seguridad.

## 6. POLÍTICAS ESPECÍFICAS

En aras de establecer los controles necesarios para cumplir con las políticas generales se generan políticas específicas, las cuales podrán contar con procedimientos, lineamientos o directrices con el fin de que sea claro para todo el personal de la organización:

- **Acuerdos de confidencialidad.**
- **Riesgos relacionados con terceros.**
- **Uso adecuado de los activos.**
- **Acceso a Internet.**
- **Correo electrónico.**

- **Recursos tecnológicos.**
- **Seguridad del Recurso Humano.**
- **Control de acceso físico.**
- **Protección y ubicación de los equipos.**
- **Segregación de funciones.**
- **Protección contra software malicioso.**
- **Copias de respaldo.**
- **Gestión de medios removibles.**
- **Intercambio de información.**
- **Control de acceso lógico.**
- **Gestión de contraseñas de usuario.**
- **Escritorio y pantalla limpia.**
- **Segregación de redes.**
- **Identificación de requerimientos de seguridad.**
- **Política de seguridad de Recursos Humanos.**
- **Política de Tratamiento de Datos Personales.**

Maria Fernanda Bertel Puyo

Firmado digitalmente por Maria Fernanda Bertel Puyo
Fecha: 2023.12.01 16:46:29 -05'00'

_____

**Gerente Gerencial**