TECNOLOGÍAS

POLÍTICA DE SEGURIDAD DIGITAL (MGRSD) MIPG

Comprende el conjunto de lineamientos para la prevención y control de los **riesgos asociados a la seguridad digital en la Entidad**, que se pueden presentar con el uso de sistemas informáticos.

Su objetivo es fortalecer la capacidad para **reconocer, gestionar y mitigar de forma efectiva** los riesgos de seguridad digital que puedan surgir durante el desarrollo de actividades cotidianas en entornos digitales y por medio de herramientas tecnológicas.

Líderes de la Política de Seguridad Digital

En la Alcaldía lo lidera el **Departamento Administrativo de Tecnologías de la Información y las Comunicaciones - DATIC.**

A nivel nacional la lidera el **Ministerio de Tecnologías de la Información y las Comunicaciones**

Sustento Normativo de la Política de Seguridad Digital

Resolución No. 00500 de marzo 10 de 2021, expedida por el Ministerio de Tecnologías de la Información y las Comunicaciones. *"Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital"*

Directiva Presidencial 03 de 2021. Lineamientos para el uso de servicios en la nube, inteligencia artificial, seguridad digital y gestión de datos.

Directiva Presidencial 02 de 2022. Reiteración de la política pública en materia de seguridad digital.

CONPES 3854 DE 2016. "Política de Seguridad Digital"

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Establece lineamientos, basados en la NTC ISO/IEC 27001, orientados a **prevenir y controlar incidentes, con el propósito de conservar la integridad, confidencialidad y disponibilidad de los activos de información** de la entidad, y minimizar la posibilidad de ocurrencia de delitos informáticos.

Sus objetivos son:

- Gestionar los riesgos asociados a los activos de información.
- Gestionar el inventario de los activos.
- Gestionar las vulnerabilidades identificadas.
- Minimizar el posible impacto de las amenazas identificadas.
- Fortalecer la cultura de seguridad de la información.

Aplica para **todos los usuarios internos en todos los niveles jerárquicos, usuarios externos, proveedores y terceros**; que produzcan, administren, custodien o que tengan acceso a la información de la Administración Central de Santiago de Cali Distrito Especial.

Líderes de Seguridad de la Información

El **Departamento Administrativo de Tecnologías de la Información y las Comunicaciones,** es el líder de la Seguridad Informática.

El **Departamento Administrativo de Desarrollo e Innovación Institucional**, mediante la Subdirección de Trámites, Servicios y Gestión Documental, lidera la Seguridad de la Información.

Sustento Normativo de la Política de Seguridad de la Información

Decreto 1078 de 2015 "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones".

Decreto 1499 de 2019 "Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015" – Artículo 2.2.22.1.5. "Articulación y complementariedad con otros sistemas de gestión".

Modelo Integrado de Planeación y Gestión MIPG - Norma Técnica Colombiana NTC ISO/IEC 27001.

¿CONOCES LAS DIFERENCIAS ENTRE ESTAS POLÍTICAS?

Política de Seguridad Digital	Política de Seguridad de la Información
Política de gestión que por medio de lineamientos para la administración del riesgo, persigue la protección de la información digital contenida en sistemas informáticos, equipos de cómputo, aplicativos, correos electrónicos, entre otros, con la finalidad de evitar la materialización de un riesgo que pueda afectar el sistema informático y su información.	Documento con alcance específico, que se centra en la protección de la información de la entidad independiente del medio donde se encuentre, sea digital, física o conocimiento, mediante la adopción de medidas preventivas, detectivas y restrictivas, en aras de garantizar su confidencialidad, disponibilidad e integridad.

Un activo de información es...

Todo recurso, herramienta o elemento que contenga **datos o información relevante para los procesos de la entidad** y que tenga valor para la Administración Central de Santiago de Cali Distrito Especial, incluyendo sistemas, hardware, software, edificios, personas, imagen corporativa e información física.

Un delito informático es...

Una actividad realizada por una o más personas, que supone una prohibición normativa, **desarrollada con el objeto de obtener provecho,** afectar la confidencialidad, integridad y disponibilidad de la información y los sistemas informáticos donde ella reposa.

En la Política de Seguridad de la Información se establecen los deberes y responsabilidades de acuerdo a los diferentes roles que intervienen en el uso de los recursos tecnológicos de la entidad.

- Ordenador del gasto
- Administradores de los centros de procesamiento de datos
- Administradores de los centros de cableado
- Encargado del retiro o traslado de los equipos de cómputo
- Administradores de recursos informáticos
- Administrador del sistema de antivirus
- Delegado del Comité Tecnológico Operativo
- Usuarios de equipos de cómputo, sistema y/o correo electrónico
- Funcionarios y Contratistas
- Subdirección de Tecnología Digital
- Encargado de los Backup
- Responsable de la adquisición de bienes y servicios
- Responsable de desarrollo de sistemas de la información
- Usuarios con incidentes informáticos

Puedes revisar la política y consultar los deberes y responsabilidades en ella, de acuerdo con el rol que desempeñas en la alcaldía.

https://sig.cali.gov.co/app.php/staff/document/viewPublic?index=1195

ALCALDÍA DE SANTIAGO DE CALI