La presente política de seguridad de la información aplica a los sistemas de información y servicios prestados por las unidades operativas de GRUPO CERCO:

- **CERCO**: Sistemas de información que soportan servicios de vigilancia y protección de bienes, establecimientos, espectáculos, certámenes y convenciones.
- **PLANISEG**: Sistemas de información que soportan servicios de portería, control de accesos e información al público, así como servicios auxiliares para tareas administrativas, archivo y similares.

Esta política tiene como objetivo establecer las directrices para garantizar la confidencialidad, integridad y disponibilidad de la información, así como proteger los datos frente a accesos no autorizados, pérdida, alteración o divulgación indebida.

Es aplicable a todos los empleados, colaboradores, contratistas y terceros que manejen o tengan acceso a la información de la organización, sin importar el medio, formato o ubicación de dicha información. Su cumplimiento es obligatorio y forma parte del compromiso institucional con la gestión segura de los activos de información.

Se establecen los principios, responsabilidades y controles necesarios para proteger la información de la organización frente a amenazas internas o externas, accidentales o deliberadas, garantizando su confidencialidad, integridad y disponibilidad. Adicionalmente, se busca:

- Fomentar una cultura organizacional de seguridad de la información.
- Cumplir con los requisitos legales y contractuales relacionados con la protección de datos.
- Promover la mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI).

La política se basa en los siguientes tres principios fundamentales:

- **Confidencialidad**: Asegurar que la información esté accesible únicamente a las personas autorizadas.
- **Integridad**: Proteger la exactitud y completitud de la información frente a modificaciones no autorizadas.
- **Disponibilidad**: Garantizar que la información esté disponible y accesible cuando sea requerida por las funciones operativas autorizadas.

Todos los empleados y terceros son responsables de proteger los datos que manejan. La Dirección asegura los recursos y la formación necesaria para mantener la seguridad. Se realizan evaluaciones de riesgos periódicas como parte de un proceso de mejora continua y en cumplimiento de normativas de RGPD y la ISO/IEC 27001. Se implementan controles técnicos y físicos, como contraseñas seguras, cifrado de datos, software actualizado y protección de documentos y equipos. El incumplimiento de esta política puede conllevar sanciones disciplinarias y legales.