# POLÍTICA DE
# SEGURIDAD DIGITAL

# OBJETIVO

Establecer las directrices para reconocer, administrar, abordar y reducir los riesgos y amenazas que puedan impactar la seguridad digital y la utilización de las TIC en ACTIVA.

# ALCANCE

El propósito de esta política es resguardar la información de la Entidad, reducir al mínimo los riesgos y garantizar la continuidad del servicio en ACTIVA.

# FUNDAMENTOS NORMATIVOS

**La presenta política se enmarca en la normatividad que a continuación se relaciona:**

• **Ley 1928 de 2018** "Por medio de la cual se aprueba el «convenio sobre la ciberdelincuencia», adoptado el 23 de noviembre de 2001, en budapest.

• **Conpes 3854 de 2016.** Política Nacional de Seguridad Digital.

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

• **Ley 1712 de 2014 .** "Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones".

• **Ley estatutaria 1581 de 2012.** Por la cual se dictan disposiciones generales para la protección de datos personales.

• **Decreto 103 de 2015.** "por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones". Derogado Parcialmente por el Decreto 1081 de 2015. • Ley 1273 de 2009. "Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones".

• **Norma Técnica Colombiana NTC ISO 27000:2013**: Requisitos para la Tecnología de la información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información.

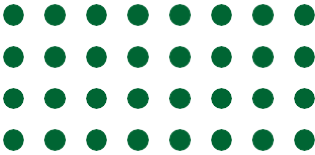
# POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La Empresa de Parques y Eventos de Antioquia - ACTIVA adopta el Modelo Nacional de Gestión de Riesgos de Seguridad Digital (MGRSD) para fortalecer la seguridad digital. Este enfoque implementa principios como la salvaguarda de derechos humanos, la responsabilidad compartida y una gestión basada en riesgos. La organización integrará estos principios en sus planes y procesos, reconociendo la importancia de abordar la incertidumbre y tomar decisiones informadas.

La implementación se realizará mediante una planificación detallada. Desde el compromiso de la alta dirección hasta la definición de roles y responsabilidades, la Empresa de Parques y Eventos de Antioquia - ACTIVA establecerá un marco de acción. Se identificarán activos de información y se aplicarán estándares de seguridad para proteger la información y la integridad de los procesos. Adicionalmente, se adoptarán estrategias externas y se controlará la operación de los sistemas para asegurar la disponibilidad y continuidad del servicio, esta estrategia quedará plasmada en el Plan estratégico de tecnologías de la información PETI.

La metodología de la Empresa de Parques y Eventos de Antioquia - ACTIVA se basa en el monitoreo y la revisión constantes. La organización realizará un seguimiento de los riesgos, evaluando su impacto y la efectividad de los controles. Buscará integrar la rendición de cuentas de la Gobernación de Antioquia, estableciendo indicadores para medir el desempeño de sus iniciativas. Las auditorías internas contribuirán a mantener la conformidad con los estándares e identificar áreas de mejora.

El enfoque de mejora continua en la gestión de riesgos de seguridad digital se traduce en acciones específicas. Mediante el Plan de Seguridad y Privacidad de la Información se abordarán hallazgos y no conformidades. La Empresa de Parques y Eventos de Antioquia - ACTIVA diseñará y ejecutará acciones para disminuir las causas subyacentes, asegurando una adaptación eficaz a los desafíos del entorno digital.



La empresa, al adoptar el MGRSD, se compromete con un ciclo proactivo de gestión de la seguridad digital. Este modelo, que abarca desde la planificación y la implementación de controles hasta el monitoreo constante y la mejora continua, permite a la organización proteger sus activos de información, asegurar la continuidad de sus operaciones y adaptarse a un panorama de amenazas en evolución, fortaleciendo así la confianza de sus usuarios y la integridad de sus servicios.

## Control de versiones

| Versión | Fecha | Descripción |
|---|---|---|
| V1 | Noviembre 2023 | Implementación de la política |
| V2 | Enero 2025 | Ampliación política |

## Aprobación

| Elaboró | Revisó | Aprobó |
|---|---|---|
| Victor Daniel Lezcano | Cristian Mauricio Buriticá García | Cristian Mauricio Buriticá García |