



Política de Seguridad Digital

Código: MIPG-M10 · Versión: 05 · Fecha: 06/09/2026

Empresa de Parques y Eventos de Antioquia – ACTIVA · NIT 901.437.957-8

1. 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.

2. 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. Aplica a todos los servidores públicos, contratistas y terceros que accedan a los activos de información de la entidad, en concordancia con el Modelo de Seguridad y Privacidad de la Información (MSPI).

3. Políticas de operación

- 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 los 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 entidad establecerá un marco de acción, identificará sus activos de información y aplicará estándares de seguridad para proteger la información y la integridad de los procesos.
- 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 entidad se basa en el monitoreo y la revisión constantes: se realizará seguimiento de los riesgos, evaluando su impacto y la efectividad de los controles; se buscará integrar la rendición de cuentas ante la Gobernación de Antioquia, estableciendo indicadores para medir el desempeño de las iniciativas, y 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 los hallazgos y no conformidades, y la entidad diseñará y ejecutará acciones para disminuir las causas subyacentes, asegurando una adaptación eficaz a los desafíos del entorno digital.
- Al adoptar el MGRSD, la entidad se compromete con un ciclo proactivo de gestión de la seguridad digital que abarca desde la planificación y la implementación de controles hasta el monitoreo constante y la mejora

continúa, lo que le permite 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.

4. Normatividad

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

- Ley 1273 de 2009. Por medio de la cual se modifica el Código Penal y se crea el bien jurídico tutelado denominado «de la protección de la información y de los datos», preservando integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones (delitos informáticos).
- Ley estatutaria 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales.
- 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.
- Decreto 1081 de 2015. Decreto Único Reglamentario del Sector Presidencia de la República, que compiló la reglamentación de la Ley 1712 de 2014 contenida en el Decreto 103 de 2015.
- 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 2017. Por medio del cual se actualiza el Modelo Integrado de Planeación y Gestión (MIPG), del cual hace parte la política de gestión y desempeño institucional de Seguridad Digital.
- 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.
- Documento CONPES 3995 de 2020. Política Nacional de Confianza y Seguridad Digital, que actualizó la Política Nacional de Seguridad Digital del CONPES 3854 de 2016.
- Resolución MinTIC 500 de 2021. Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el Modelo de Seguridad y Privacidad de la Información (MSPI) como habilitador de la política de Gobierno Digital; modificada por la Resolución MinTIC 746 de 2022.
- Decreto 338 de 2022. Por el cual se adiciona el Título 21 a la Parte 2 del Libro 2 del Decreto 1078 de 2015 y se establecen los lineamientos generales para fortalecer la gobernanza de la seguridad digital, la identificación de infraestructuras críticas cibernéticas y la gestión de incidentes de seguridad digital.
- Decreto 767 de 2022. Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015.
- Norma Técnica NTC-ISO/IEC 27001:2022. Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de Gestión de la Seguridad de la Información. Requisitos.

5. Lineamientos

- Adoptar e implementar el Modelo de Seguridad y Privacidad de la Información (MSPI) del Ministerio de Tecnologías de la Información y las Comunicaciones como marco de referencia para la gestión de la seguridad digital de la entidad.
- Gestionar los riesgos de seguridad digital conforme al Modelo Nacional de Gestión de Riesgos de Seguridad Digital (MGRSD) y a la Guía para la Administración del Riesgo del DAFP, integrándolos al mapa de riesgos institucional.
- Mantener actualizado el inventario y la clasificación de los activos de información, aplicando controles de seguridad acordes con su criticidad.

- Reportar y gestionar los incidentes de seguridad digital y, cuando corresponda, escalarlos a las instancias de gobernanza de seguridad digital del Gobierno Nacional previstas en el Decreto 338 de 2022.
- Promover la cultura de seguridad digital mediante actividades de sensibilización y capacitación dirigidas a servidores públicos y contratistas.
- Articular esta política con la política de Gobierno Digital, el PETI, el Plan de Seguridad y Privacidad de la Información y el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.

6. Responsabilidades

- Alta dirección (Gerencia General): demuestra compromiso con la seguridad digital, asigna los recursos necesarios y respalda la implementación de la política.
- Comité Institucional de Gestión y Desempeño (Resolución 015 de 2022): orienta, revisa, aprueba y hace seguimiento a la política y a sus planes derivados.
- Proceso TIC: lidera la implementación del MSPI, del PETI y del Plan de Seguridad y Privacidad de la Información, y gestiona los incidentes de seguridad digital.
- Jefatura de Control Interno: evalúa de manera independiente la implementación de la política mediante auditorías internas.
- Servidores públicos, contratistas y terceros: cumplen las directrices de seguridad digital, hacen uso adecuado de los activos de información y reportan oportunamente los incidentes o debilidades de seguridad que identifiquen.

7. Seguimiento y evaluación

El seguimiento a esta política se realizará a través de los indicadores definidos en el Plan de Seguridad y Privacidad de la Información y en el PETI, de las auditorías internas, del autodiagnóstico de la política de Seguridad Digital del MIPG y del reporte anual del Formulario Único de Reporte de Avances de la Gestión (FURAG). Los resultados se presentarán al Comité Institucional de Gestión y Desempeño, que definirá las acciones de mejora continua a que haya lugar.

8. Documentos asociados

- Plan Estratégico de Tecnologías de la Información (PETI)
- Plan de Seguridad y Privacidad de la Información
- Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información (Decreto 612 de 2018)
- Política de Gobierno Digital de ACTIVA
- OE-M02 Política de Gestión del Riesgo
- Política de Uso Aceptable de Recursos Tecnológicos de ACTIVA
- Reglamento Interno de Trabajo (Resolución 202605000058 de 2026)

9. Control de versiones

Nº de Versión	Fecha de Versión	Elaborado por	Revisado por	Aprobado por	Descripción del cambio
01	Noviembre 2023	Víctor Daniel Lezcano	Cristian Mauricio Buriticá García	Cristian Mauricio Buriticá García	Implementación de la política
02	Enero 2025	Víctor Daniel Lezcano	Cristian Mauricio Buriticá García	Cristian Mauricio Buriticá García	Ampliación política

Nº de Versión	Fecha de Versión	Elaborado por	Revisado por	Aprobado por	Descripción del cambio
03	28/07/2026	Apoyo SGC	Comité Institucional de Gestión y Desempeño	Comité Institucional de Gestión y Desempeño	Actualización del marco normativo: se reemplaza el CONPES 3854 de 2016 por el CONPES 3995 de 2020 (Política Nacional de Confianza y Seguridad Digital); la cita directa al Decreto 103 de 2015 (compilado) se reemplaza por el Decreto 1081 de 2015; la referencia errónea «NTC ISO 27000:2013» se corrige por la NTC-ISO/IEC 27001:2022; se incorporan el Decreto 1499 de 2017 (MIPG), la Resolución MinTIC 500 de 2021 modificada por la Resolución 746 de 2022 (MSPI), el Decreto 338 de 2022 (gobernanza de seguridad digital) y el Decreto 767 de 2022 (Gobierno Digital). Se complementan las secciones de Lineamientos, Responsabilidades y Seguimiento y evaluación conforme al marco general MIPG/MSPI, se precisan los documentos asociados y se corrigen erratas de forma («la presenta política», «budapest» en minúscula).
04	04/09/2026	Sistema de Gestión de Calidad	Dirección Administrativa y Financiera	Comité Institucional de Gestión y Desempeño	Reedición de la política en el formato institucional del Sistema de Gestión de Calidad (SGC), sobre el texto de la versión 03 del 28/07/2026 (archivo editable «Política 10 Seguridad Digital V3.docx»), que es la versión controlada vigente. Se cotejaron ese editable y el PDF publicado en la carpeta del Modelo Integrado de Planeación y Gestión («Política de Seguridad Digital.pdf»); el PDF corresponde a la versión 02 de enero de 2025, no a la 03, de modo que no difiere de la versión 03 por discrepancias de transcripción sino por ser anterior; todo su contenido está recogido en la versión 03 con los cambios que declara la fila 03 de este control. Por eso se conserva el texto de la versión 03 y se deja constancia de que el PDF publicado debe reemplazarse por el de esta versión. Cambios: (1) el Código pasa de «MIPG» —etiqueta compartida por las diecinueve políticas del Modelo, que no individualiza el documento— a «MIPG-M10», por decisión de la entidad del 04/09/2026; la cabecera conserva «Modelo Integrado de Planeación y Gestión». (2) El título «Política de Seguridad Digital» se conserva tal como lo traen el editable y el PDF; el nombre del archivo se escribe sin tildes. (3) Se actualizan la versión (3 a 04) y la fecha (28/07/2026 a 04/09/2026) y se abre esta fila con elaboró «Sistema de Gestión de Calidad», revisó «Dirección Administrativa y Financiera» y aprobó «Comité Institucional de Gestión y Desempeño», órgano que adopta las políticas del Modelo en ACTIVA y que ya aprobó la versión 03. (4) Se repone en el apartado 4 la frase de entrada del listado normativo, que el PDF traía con la errata «La presenta política se enmarca en la

Nº de Versión	Fecha de Versión	Elaborado por	Revisado por	Aprobado por	Descripción del cambio
					normatividad que a continuación se relaciona:» y que aquí se lee «La presente política se enmarca en la normatividad que a continuación se relaciona:»; la fila 03 la da por corregida, pero en la versión 03 la frase entera había sido suprimida. (5) En el apartado 6 «Responsabilidades», por decisión de la entidad del 04/09/2026, se normalizan a la nomenclatura vigente tres denominaciones genéricas: «Alta dirección (Gerencia)» pasa a «Alta dirección (Gerencia General)», «Rol o área responsable de las tecnologías de la información» pasa a «Jefatura TIC» y «Rol de Control Interno» pasa a «Jefatura de Control Interno»; las funciones descritas para cada uno no cambian. (6) En las filas 01 y 02 de este control la casilla «Descripción del cambio» se repone con la grafía literal del PDF publicado («Implementación de la política» y «Ampliación política»), que la versión 03 había transcrito como «Creación del documento (implementación de la política).» y «Ampliación de la política.»; los nombres de las casillas Elaborado, Revisado y Aprobado de esas dos filas proceden del bloque único de aprobación del PDF, tal como los distribuyó la versión 03, y se conservan literales. (7) Se escriben sin espacios alrededor del guion el código «OE-M02» del apartado 8 y la designación «NTC-ISO/IEC 27001:2022» de los apartados 4 y 9, gráficas normalizadas del código del SGC y de la norma ICONTEC. Salvo la frase repuesta en el apartado 4, los tres cargos normalizados en el apartado 6 y las gráficas del punto (7), el objetivo, el alcance, las seis políticas de operación, las doce normas, los seis lineamientos, las cinco responsabilidades, el seguimiento y evaluación y los siete documentos asociados se conservan literales respecto de la versión 03; la fila 03 de este control se conserva literal.
05	06/09/2026	Sistema de Gestión de Calidad	Dirección Administrativa y Financiera	Gerencia General	Corrección de la denominación del cargo, conforme al organigrama vigente, que no contempla una Jefatura TIC: el cargo de la planta es el Profesional TIC, adscrito a la Dirección Administrativa y Financiera, y cuando el texto alude al área o a la función se escribe «Proceso TIC». (1) Apartado 6 «Responsabilidades»: la viñeta «Jefatura TIC: lidera la implementación del MSPI, del PETI y del Plan de Seguridad y Privacidad de la Información, y gestiona los incidentes de seguridad digital.» pasa a «Proceso TIC: lidera la implementación del MSPI, del PETI y del Plan de Seguridad y Privacidad de la Información, y gestiona los incidentes de seguridad digital.»; sólo cambia la denominación inicial y el resto de la viñeta queda literal. Es la única aparición de «Jefatura TIC» en el cuerpo

Nº de Versión	Fecha de Versión	Elaborado por	Revisado por	Aprobado por	Descripción del cambio
					del documento. El punto (5) de la descripción del cambio de la versión 04, en el apartado 9, se conserva literal por ser el registro de lo actuado entonces: aquella entrega sustituyó «Rol o área responsable de las tecnologías de la información» por «Jefatura TIC», y es esa sustitución la que ahora se corrige. Salvo lo indicado, el resto del documento se conserva literal.