Empresa Social del Estado
HOSPITAL MENTAL DE ANTIOQUIA
— María Upegui —
HOMO

RESOLUCIÓN

202620468
Radicado Nro 202620468
Bello, 2026-11-11 16:57:00

"Por medio de la cual se adoptan la Política de Gobierno Digital, la Política de Seguridad Digital y la Política de Autorización y Protección de Datos Personales, y se establece la Estrategia Institucional de Seguridad Digital de la E.S.E. Hospital Mental de Antioquia María Upegui – HOMO"

LA GERENTE DE LA EMPRESA SOCIAL DEL ESTADO HOSPITAL MENTAL DE ANTIOQUIA MARÍA UPEGUI – HOMO, en ejercicio de sus atribuciones legales y estatutarias, en especial las conferidas por la Ley 100 de 1993, la Ordenanza 17 de 1994, los Decretos 1876 de 1994 y 139 de 1996, el Acuerdo 026 de 1996 – Estatutos Internos, y

CONSIDERANDO:

1. Que los artículos 15 y 20 de la Constitución Política reconocen, respectivamente, los derechos a la intimidad, al buen nombre y al hábeas data, así como las libertades de expresión e información, garantías que deben armonizarse con el acceso a la información pública previsto en el artículo 74 superior.

2. Que los artículos 209 y 269 de la Constitución Política disponen que la función administrativa se desarrolla al servicio de los intereses generales con fundamento en los principios allí previstos y que las entidades públicas deben diseñar y aplicar métodos y procedimientos de control interno.

3. Que los artículos 194 y 195 de la Ley 100 de 1993 regulan la naturaleza y el régimen jurídico de las Empresas Sociales del Estado, entidades públicas descentralizadas con personería jurídica, patrimonio propio y autonomía administrativa, sujetas a las disposiciones especiales que las rigen.

4. Que la E.S.E. Hospital Mental de Antioquia María Upegui – HOMO fue transformada en Empresa Social del Estado mediante la Ordenanza 17 de 1994 y se rige, entre otras disposiciones, por el Decreto 1876 de 1994, el Decreto 139 de 1996 y sus Estatutos Internos, normas que deben interpretarse de manera armónica para el ejercicio de las funciones de dirección y representación legal de la Gerencia.

5. Que la Ley 1341 de 2009, modificada por la Ley 1978 de 2019, establece el marco general del sector de las tecnologías de la información y las comunicaciones y orienta el aprovechamiento de las TIC para el desarrollo de las funciones públicas.

6. Que el Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, en el capítulo 1 del título 9 de la parte 2 del libro 2, subrogado por el Decreto 767 de 2022, establece los lineamientos generales de la Política de Gobierno Digital y dispone que el representante legal es responsable de coordinar, adoptar, implementar y hacer seguimiento y verificación de su implementación, mientras que el responsable de TIC lidera su implementación y mejora continua.

7. Que el Decreto 1499 de 2017, incorporado en el Decreto 1083 de 2015, regula el Modelo Integrado de Planeación y Gestión – MIPG y asigna al Comité Institucional de Gestión y Desempeño funciones de orientación, articulación y seguimiento, incluida la implementación y desarrollo de las políticas y directrices en materia de seguridad digital y de la información, en los términos de su ámbito de aplicación.

8. Que el Decreto 338 de 2022 estableció lineamientos para fortalecer la gobernanza de la seguridad digital, la gestión de riesgos, la identificación y reporte de infraestructuras críticas cibernéticas y servicios esenciales, así como la gestión y respuesta a incidentes de seguridad digital.

9. Que el parágrafo del artículo 16 del Decreto Ley 2106 de 2019 prevé que las autoridades que realicen trámites, procesos y procedimientos por medios digitales deben contar con una estrategia de seguridad digital para la gestión documental electrónica y la preservación de la información, conforme a los lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones.

10. Que la Resolución 500 de 2021 del Ministerio de Tecnologías de la Información y las Comunicaciones estableció lineamientos y estándares para la Estrategia de Seguridad Digital y adoptó el Modelo de Seguridad y Privacidad de la Información – MSPI como habilitador de la Política de Gobierno Digital; su artículo 5 dispone que la estrategia integre políticas, procedimientos, guías, manuales, formatos y lineamientos y se incorpore en el Plan de Seguridad y Privacidad de la Información.

11. Que la Resolución 746 de 2022 fortaleció el MSPI y estableció lineamientos adicionales, y que la Resolución 2277 de 2025 actualizó el Anexo 1 de la Resolución 500 de 2021, por lo que la implementación institucional debe sujetarse al anexo actualizado y a los lineamientos técnicos vigentes que expida MinTIC.

12. Que la Ley Estatutaria 1581 de 2012 y su reglamentación compilada en el Decreto 1074 de 2015 establecen el régimen general de protección de datos personales, incluidos los principios, derechos de los titulares, deberes de responsables y encargados, reglas sobre datos sensibles y el principio de responsabilidad demostrada.

13. Que la Ley 1712 de 2014 regula la transparencia y el derecho de acceso a la información pública y exige armonizar la divulgación de información con las excepciones legales relativas a datos personales, información clasificada y reservada.

14. Que, por la naturaleza asistencial de la E.S.E., el tratamiento de información en salud y la administración de historias clínicas deben observar, además, la Ley 23 de 1981, la Ley Estatutaria 1751 de 2015, la Ley 2015 de 2020, la Resolución 1995 de 1999 y su modificación por la Resolución 839 de 2017, así como las demás disposiciones sectoriales aplicables.

15. Que la Ley 1273 de 2009 incorporó disposiciones penales para la protección de la información y de los datos, y la Ley 594 de 2000, junto con el Decreto 1080 de 2015, establece reglas para la gestión, conservación y preservación documental.

16. Que el Decreto 0385 del 7 de abril de 2026 sustituyó el título de directrices generales de técnica normativa del Decreto 1081 de 2015 y establece, entre otros aspectos, la observancia de la jerarquía normativa, la motivación suficiente, la coordinación, la claridad, precisión, sencillez y coherencia, la estructura del acto administrativo y la identificación expresa de las disposiciones que se derogan o modifican, en los términos aplicables a las entidades territoriales.

17. Que la E.S.E. actualizó la Política de Gobierno Digital, código GE-PE-PO-21, versión 02; la Política de Seguridad Digital, código GE-PE-PO-22, versión 02; y la Política de Autorización y Protección de Datos Personales, código GE-PE-PO-23, versión 02, todas con fecha 26 de febrero de 2026, documentos que contienen lineamientos institucionales para la transformación digital, la gestión de riesgos de seguridad digital y el tratamiento de datos personales.

18. Que las políticas institucionales fueron sometidas a revisión y orientación del Comité Institucional de Gestión y Desempeño, según consta en el Acta No.06 del 05 de agosto de 2026, documento que reposa en la oficina de planeación y el sistema de Almera.

19. Que, en consecuencia, se requiere adoptar formalmente las políticas institucionales indicadas, definir sus responsabilidades y articular su implementación con los instrumentos de planeación, gestión documental, seguridad de la información, protección de datos y mejoramiento institucional de la E.S.E.

En mérito de lo expuesto,

RESUELVE

ARTÍCULO PRIMERO. Adoptar para la E.S.E. Hospital Mental de Antioquia María Upegui – HOMO las siguientes políticas institucionales: (i) Política de Gobierno Digital; (ii) Política de Seguridad Digital; y (iii) Política de Autorización y Protección de Datos Personales. Estas políticas establecen los lineamientos institucionales para el uso estratégico de las TIC, la transformación digital, la protección de los activos de información, la gestión de riesgos de seguridad digital y el tratamiento lícito y seguro de los datos personales.

ARTÍCULO SEGUNDO. Identificación e incorporación de los documentos adoptados. Incorporar como anexos integrantes de la presente resolución, y parte integral de la misma, los siguientes documentos institucionales:

1. Política de Gobierno Digital, código GE-PE-PO-21, versión 02, del 26 de febrero de 2026 (Anexo 1).

2. Política de Seguridad Digital, código GE-PE-PO-22, versión 02, del 26 de febrero de 2026 (Anexo 2).

3. Política de Autorización y Protección de Datos Personales, código GE-PE-PO-23, versión 02, del 26 de febrero de 2026 (Anexo 3).

PARÁGRAFO. Los documentos relacionados deberán adjuntarse efectivamente a la presente resolución, conservar su identificación, código, versión y fecha de aprobación, y reposar en el Sistema Integrado de Gestión de la entidad, conforme a los procedimientos institucionales de gestión y control documental.

ARTÍCULO TERCERO. Estrategia Institucional de Seguridad Digital. Establecer la Estrategia Institucional de Seguridad Digital de la E.S.E., articulada con la Política de Gobierno Digital y sustentada en la Política de Seguridad Digital y la Política de Autorización y Protección de Datos Personales. La estrategia se implementará de conformidad con la Resolución MinTIC 500 de 2021, sus modificaciones y el Anexo 1 actualizado por la Resolución 2277 de 2025.

La estrategia se desarrollará mediante los instrumentos técnicos y administrativos institucionales vigentes, según su código y versión en el Sistema Integrado de Gestión, incluyendo, cuando existan y se encuentren aprobados: (i) Plan de Seguridad y Privacidad de la Información; (ii) Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información; (iii) procedimiento de gestión, reporte, respuesta y recuperación frente a incidentes; (iv) inventario y clasificación de activos de información; (v) controles de acceso, continuidad y respaldo; y (vi) actividades de formación y sensibilización.

PARÁGRAFO 1. El Plan de Seguridad y Privacidad de la Información deberá incorporar la estrategia y articularse con el Plan de Acción institucional, de conformidad con las disposiciones aplicables.

PARÁGRAFO 2. La referencia a los instrumentos señalados en el presente artículo no implica la adopción de documentos que no hayan sido formalmente aprobados conforme al procedimiento institucional de control documental. Corresponderá al proceso de Gestión de Tecnologías de la Información y las Comunicaciones (TIC) verificar su existencia y pertinencia técnica, en el ámbito de sus competencias, en articulación con los responsables del Sistema Integrado de Gestión, a quienes corresponderá lo relacionado con su vigencia, codificación y control documental.

ARTÍCULO CUARTO. Ámbito de aplicación. Las políticas y la estrategia serán aplicables a todos los procesos estratégicos, misionales, de apoyo y de evaluación de la E.S.E. y a los servidores públicos, contratistas, estudiantes, practicantes, proveedores y demás terceros, en cuanto accedan, administren, custodien, procesen, transmitan o utilicen activos de información, sistemas, infraestructura tecnológica o datos personales bajo responsabilidad de la entidad.

Los pacientes, usuarios, familiares y ciudadanía ejercerán sus derechos y utilizarán los canales digitales conforme a las reglas de acceso, privacidad, seguridad y protección de datos que les resulten aplicables.

ARTÍCULO QUINTO. Responsabilidades institucionales. La implementación y seguimiento de las políticas se cumplirán de acuerdo con las competencias y funciones institucionales:

1. Gerencia. Como representante legal y responsable institucional de la Política de Gobierno

Digital, coordinará su adopción, implementación, seguimiento y verificación; promoverá la articulación de las políticas y dispondrá las decisiones administrativas que correspondan dentro de sus competencias.

2. Comité Institucional de Gestión y Desempeño. Orientará la implementación, articulará las acciones institucionales, conocerá los resultados de seguimiento y formulará recomendaciones de mejora, conforme a sus funciones legales y reglamentarias.

3. Proceso de Gestión de Tecnologías de la Información y las Comunicaciones – TIC. Liderará la implementación y mejora continua de la Política de Gobierno Digital y coordinará técnicamente los instrumentos del Modelo de Seguridad y Privacidad de la Información (MSPI), en articulación con la Dirección Técnica de Planeación y las demás dependencias competentes, para garantizar su adecuada implementación y seguimiento institucional.

4. Responsable de Seguridad de la Información o quien haga sus veces. Coordinará, dentro de las funciones que le sean asignadas, la gestión de riesgos, controles, incidentes, sensibilización y seguimiento del MSPI. Su designación no crea por sí misma un empleo, dependencia o asignación salarial.

5. Dependencia o servidor responsable de protección de datos personales. Coordinará el cumplimiento del régimen de protección de datos, la atención de consultas y reclamos y la articulación con los responsables de las bases de datos y procesos que traten información personal.

6. Líderes de proceso. Identificarán y protegerán los activos de información bajo su responsabilidad, aplicarán controles y garantizarán que el tratamiento de datos se realice conforme a las finalidades y competencias del proceso.

7. Servidores públicos, trabajadores oficiales, contratistas y terceros. Cumplirán las políticas, procedimientos, controles y obligaciones de confidencialidad que les resulten aplicables según sus funciones, contratos, convenios o acceso a información.

8. Oficina de Control Interno. Evaluará de manera independiente el diseño y efectividad de los controles, dentro del marco de sus competencias, sin asumir funciones de ejecución o administración de los controles.

ARTÍCULO SEXTO. Implementación, seguimiento y articulación con la planeación institucional. La implementación de las políticas y la estrategia adoptadas mediante la presente resolución se desarrollará de manera articulada entre la Dirección Técnica de Planeación y el proceso de Gestión de Tecnologías de la Información y las Comunicaciones (TIC), de conformidad con sus respectivas competencias.

La Dirección Técnica de Planeación, en ejercicio del liderazgo institucional del Modelo de Seguridad y Privacidad de la Información (MSPI), orientará y coordinará su implementación y seguimiento institucional, conforme a lo establecido en la Resolución 0385 de 2025. Por su parte, el proceso de Gestión TIC ejercerá el liderazgo técnico y tecnológico, apoyando la implementación y mejora continua de la Política de Gobierno Digital y coordinando los instrumentos técnicos del MSPI, en articulación con Planeación y las demás dependencias

competentes.

Para tal efecto, se definirán los responsables, cronogramas, indicadores, fuentes de verificación y mecanismos de seguimiento y reporte, de acuerdo con los instrumentos de planeación institucional vigentes.

Los avances en la implementación de las políticas y los riesgos identificados serán presentados periódicamente al Comité Institucional de Gestión y Desempeño, para su conocimiento, orientación y seguimiento, conforme a sus competencias.

ARTÍCULO SÉPTIMO. Recursos y sostenibilidad. La implementación se desarrollará con los recursos humanos, técnicos, tecnológicos, logísticos y financieros que sean aprobados para la entidad, de acuerdo con la disponibilidad presupuestal, la planeación institucional, las reglas presupuestales y las competencias de las instancias correspondientes. La presente resolución no constituye por sí misma autorización de gasto, modificación presupuestal ni compromiso de recursos no apropiados.

ARTÍCULO OCTAVO. Protección de datos personales e información clínica. La E.S.E. garantizará la protección, confidencialidad, custodia y tratamiento adecuado de los datos personales y de la información clínica, conforme a la Constitución Política, la Ley 1581 de 2012, el Decreto 1074 de 2015, la Ley 23 de 1981, la Ley 1751 de 2015, la Ley 2015 de 2020, la Resolución 1995 de 1999, la Resolución 839 de 2017 y demás normas concordantes.

La entrega de copias de historias clínicas y certificados de diagnóstico se realizará conforme a las disposiciones legales y jurisprudenciales aplicables y al procedimiento institucional establecido como requisitos para su solicitud, atendiendo la calidad del solicitante, la acreditación del parentesco o representación, las autorizaciones correspondientes y los requerimientos de autoridades judiciales, administrativas y de salud, según sus competencias legales.

PARÁGRAFO. La entrega de esta información deberá garantizar la verificación de la legitimidad de la solicitud, su finalidad y la habilitación legal correspondiente, preservando en todo momento la reserva de la historia clínica y los derechos de sus titulares.

ARTÍCULO NOVENO. Divulgación y apropiación. El proceso de Gestión TIC, con el apoyo de la Dirección Técnica de Planeación, Gestión Humana, Comunicaciones y demás dependencias competentes, adelantará acciones de divulgación, capacitación y sensibilización para promover el conocimiento y aplicación de las políticas.

Las obligaciones de seguridad, confidencialidad, privacidad, gestión de incidentes y devolución o eliminación de información deberán incorporarse, cuando resulte procedente, en los contratos, convenios, acuerdos de confidencialidad y demás instrumentos que habiliten a terceros para acceder o tratar información institucional.

ARTÍCULO DÉCIMO. Revisión y actualización. Las políticas se revisarán cuando se presenten cambios normativos, tecnológicos, organizacionales, asistenciales, operativos o de riesgos que afecten su contenido o aplicación, y al menos con la periodicidad definida en el procedimiento institucional de control documental.

Las modificaciones sustanciales deberán someterse a revisión y orientación del Comité Institucional de Gestión y Desempeño y ser adoptadas por la Gerencia mediante el acto administrativo correspondiente. Los instrumentos operativos podrán actualizarse por el procedimiento de control documental, siempre que no alteren el objeto, alcance o lineamientos esenciales de las políticas.

ARTÍCULO DÉCIMO PRIMERO. Publicación y vigencia. La presente resolución se publicará por el medio oficial que resulte jurídicamente procedente para la E.S.E., de conformidad con el artículo 65 de la Ley 1437 de 2011, modificado por la Ley 2080 de 2021. Adicionalmente, se divulgará en la sede electrónica o página web institucional y en los canales internos dispuestos para tal fin.

La resolución rige a partir de su publicación, sin perjuicio de las actividades de implementación y divulgación que deban ejecutarse con posterioridad.

PUBLÍQUESE, COMUNÍQUESE Y CÚMPLASE.
Dada en Medellín, a los diez (10) días del mes de noviembre de 2026.

ADRIANA PATRICIA ROJAS ESLAVA
Gerente

	Nombre	Cargo	Firma	Fecha
Elaboro y actualizó el componente jurídico	Carolina Montes Franco	Abogada – Defensa Jurídica		10-11-2026
Elaboro y actualizó los componentes técnicos y tecnológicos	Mauricio Pulgarín Gallego	Profesional Universitario – Gestión TIC		10-11-2026
Revisó y aprobó el componente jurídico	Wilmar Estik Gómez Villa	Jefe Oficina Jurídica		10-11-2026
Revisó y aprobó planeación y estrategia	Duber Mary Velasquez Alzate	Directora Técnica de Planeación y Proyectos -Oficial de Cumplimiento		10-11-2026
Revisó avaló y aprobó	Juan Santiago Puentes Echeverri	Subgerente Administrativo y Financiero		10-11-2026
Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a la normas y disposiciones legales vigentes y, por tanto, bajo nuestra responsabilidad lo presentamos para firma.				