Empresa Social del Estado
HOSPITAL MENTAL DE ANTIOQUIA
HOMO

POLITICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Contenido

1. INTRODUCCIÓN

La dirección de la E.S.E Hospital Mental de Antioquia, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un sistema de gestión de seguridad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y la visión de la Entidad.

El presente documento contiene las políticas de seguridad de la información y las políticas de tratamiento de datos personales en cumplimiento de lo establecido en Ley 1581 de 2012 y del Decreto 1377 de 2013.

Se busca la implementación de las mejores prácticas dadas por el Departamento Administrativo de la Función Pública con su estrategia MIPG y el Ministerio de las Tecnologías de la Información y las comunicaciones en el diagnóstico, planificación, implementación, gestión y mejoramiento continuo, del Modelo de Seguridad y Privacidad de la Información.

El Modelo de Seguridad y Privacidad de la información, pretende lograr en la institución y sus clientes internos, externos y partes interesadas confianza en el manejo de la información garantizando para cada uno la privacidad, continuidad, integralidad y disponibilidad de los datos.

2. OBJETIVOS

Objetivo general

Generar un documento institucional guiado en lineamientos de buenas prácticas en seguridad y privacidad de la información y los datos personales.

Objetivos específicos

- Minimizar el riesgo en las funciones más importantes de la Entidad.
- Cumplir con los principios de seguridad y privacidad de la información.
- Cumplir con los principios de la función administrativa.

- Establecer las políticas, procedimientos e instructivos en materia de seguridad y privacidad de la información.
- Promover el uso de mejores prácticas de seguridad de la información en la institución.
- Optimizar la gestión de la seguridad de la información al interior de la entidad.
- Aplicar de manera correcta la legislación relacionada con la protección de datos personales.
- Optimizar la labor de acceso a la información pública.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes de la E.S.E Hospital Mental de Antioquia.

3. ALCANCE DEL DOCUMENTO

La política de seguridad y privacidad de la información cubre todos los aspectos administrativos y/o asistenciales que deben ser cumplidos por los directivos, funcionarios y terceros que laboren o tengan relación con la E.S.E hospital Mental de Antioquia en los diferentes procesos de la institución, para preservar la seguridad de la información de la Entidad.

El plan de riesgos de seguridad y privacidad aplica a todos los procesos de la institución los cuales manejen, procesen o interactúen con información institucional.

4. APLICABILIDAD DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Esta política aplica a toda la entidad, sus funcionarios, contratistas y terceros de la E.S.E Hospital Mental de Antioquia y la ciudadanía en general.

Todas las personas cubiertas por el alcance y aplicabilidad deberán dar cumplimiento un 100% de la política.

5. TÉRMINOS Y DEFINICIONES

Acceso a la información pública: Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4)

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas) que tenga valor para la organización (ISO/IEC27000).

Activo de Información: En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.

Archivo: Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3)

Amenazas: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

Análisis de riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000)

Auditoría: Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría (ISO/IEC 27000).

Autorización: Consentimiento previo, expreso e informado del Titular para llevar a cabo el tratamiento de datos personales (Ley 1581 de 2012, art 3).

Bases de datos personales: Conjunto organizado de datos personales que sea objeto de tratamiento (Ley 1581 de 2012, art 3).

Ciberseguridad: Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).

Ciberespacio: Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programar computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).

Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también un sinónimo de salvaguarda o contramedida. En una definición más simple es una medida que modifica el riesgo.

Datos abiertos: Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de2014, art 6).

Datos personales: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales o determinables (Ley 1581 de 2012, art 3).

Datos personales públicos: Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3).

Datos personales privados: Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal H).

Datos personales mixtos: Para efectos de esta guía es la información que contiene datos personales públicos junto con datos privados o sensibles.

Datos personales sensibles: Se entiende por datos sensibles aquellos que afectan la intimidad del titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones

religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3).

Declaración de aplicabilidad: Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información-SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001 (ISO/IEC 270000).

Derecho a la intimidad: Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permita a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural. (Jurisprudencia corte constitucional).

Encargado del tratamiento de datos: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el tratamiento de datos personales por cuenta del Responsable del Tratamiento. (Ley 1581 de 2012, art 3).

Gestión de incidentes de seguridad de la información: Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información (ISO/IEC 27000).

Información pública clasificada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).

Información pública reservada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014 (Ley 1712 de 2014, art 6).

Ley de Habeas Data: Se refiere a la ley estatutaria 1266 de 2008.

Ley de transparencia y Acceso a la Información Pública: Se refiere a la Ley Estatutaria 1712 de 2014.

Mecanismos de protección de datos personales: Lo constituyen las distintas alternativas con que cuentan las entidades destinatarias para ofrecer protección a los datos personales de los titulares tales como acceso controlado, anonimización o cifrado.

Plan de continuidad del negocio: Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro (ISO/IEC 27000).

Plan de tratamiento de riesgos: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma (ISO/IEC 27000).

Privacidad: En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del **PETIC** la correlativa obligación de proteger dicha información en observancia del marco legal vigente.

Registro Nacional de Bases de Datos: Directorio público de las bases de datos sujetas a tratamiento que operan el país (Ley 1581 de 2012, art 25).

Responsabilidad demostrada: Conducta desplegada por los responsables o encargados del tratamiento de datos personales bajo la cual a petición de la superintendencia de Industria y Comercio deben estar en capacidad de demostrarle a dicho organismo de control que han implementado medidas apropiadas y efectivas para cumplir lo establecido en la Ley 1581 de 2012 y sus normas reglamentarias.

Responsable del Tratamiento de datos: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o Tratamiento de los datos (Ley 1581 de 2012, art 3).

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias (ISO/IEC 27000).

Seguridad de la información: Preservación de la confidencialidad, integridad, y disponibilidad de la información (ISO/IEC 27000).

Sistema de Gestión de Seguridad de la Información SGSI: Conjunto de elementos interrelacionados o interactuantes (Estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua (ISO/IEC 27000).

Titulares de la información: Personas naturales cuyos datos personales sean objeto de Tratamiento (Ley 1581 de 2012, art 3).

Transferencia: La transferencia de datos tiene lugar cuando el responsable y/o encargado del tratamiento de datos personales, ubicado en Colombia, envía la información o los datos personales a un receptor, que a su vez es responsable del tratamiento y se encuentra dentro o fuera del país.

Transmisión: Tratamiento de datos personales que implica la comunicación de los mismos dentro o fuera del territorio de la República de Colombia.

Tratamiento de datos personales: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión (Ley 1581 de 2012, art 3).

Trazabilidad: Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad (ISO/IEC 27000).

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas (ISO/IEC 27000).

Partes interesadas (Stakeholder): Persona y organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

6. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

La E.S.E Hospital Mental de Antioquia, en cumplimiento estricto de las leyes y en concordancia con su misión, visión y objetivos estratégicos entiende la importancia que tiene la gestión segura de la información, por lo tanto está comprometida con la implementación de un sistema de gestión de seguridad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos.

- La E.S.E Hospital Mental de Antioquia ha decidido **definir, implementar, operar y mejorar** de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios que le aplican a su naturaleza.
- Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de **los empleados, contratistas o terceros.**
- La E.S.E Hospital Mental de Antioquia protegerá la información generada, procesada o resguardada por los procesos de negocio y activos de información que hacen parte de los mismos.
- La E.S.E Hospital Mental de Antioquia protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
- La E.S.E Hospital Mental de Antioquia protegerá su información de las amenazas originadas por parte del personal.
- La E.S.E Hospital Mental de Antioquia protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
- La E.S.E Hospital Mental de Antioquia controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
- La E.S.E Hospital Mental de Antioquia implementará control de acceso a la información, sistemas y recursos de red.
- La E.S.E Hospital Mental de Antioquia garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

- La E.S.E Hospital Mental de Antioquia garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.
- La E.S.E Hospital Mental de Antioquia garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.
- La E.S.E Hospital Mental de Antioquia garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.
- La Entidad establece roles y responsabilidades para el gobierno, la gestión, administración y operación de la seguridad de la información.
- La entidad adopta mecanismos de autenticación para el acceso y/o uso de los activos de información, los cuales son personales e intransferibles. Los servidores públicos, terceros y contribuyentes son responsables de tomar precauciones para mantener en secreto los medios de autenticación.
- La Entidad define el área responsable de autorizar la adquisición, instalación, cambio o eliminación de componentes de la plataforma tecnológica (hardware y software).
- La Entidad define su plan de continuidad de negocio con el fin de asegurar la disponibilidad de sus procesos misionales y la continuidad de su operación para que sean ejecutados por sus servidores públicos.

7. POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES

Con el propósito de dar cumplimiento a la ley estatutaria 1581 de 2012, y su decreto reglamentario 1377 de 2013, en el sentido que los datos personales pueden ser requeridos por la E.S.E Hospital Mental de Antioquia, bajo el condicionamiento que la petición se sustente en la conexidad directa con las funciones que desarrolla, este tratamiento debe ser coherente con la protección irrestricta del derecho de Hábeas data del titular de la información.

- Los datos personales proporcionados a la E.S.E Hospital Mental de Antioquia son objeto de tratamiento (recolección, almacenamiento, uso, circulación o suspensión), con el objeto de darle la finalidad específica para la que fueron suministrados y el cumplimiento de las funciones constitucionales y legales de la Entidad, según la reglamentación de la respectiva función o del servicio en virtud del cual el titular proporcionó dichos datos.
- El tratamiento de datos personales es requerido en el desarrollo de los procesos de apoyo de la Entidad específicamente los siguientes:

TALENTO HUMANO: El tratamiento de los datos se realizará para la vinculación, desempeño de funciones o prestación de servicios, retiro o terminación, dependiendo del tipo de relación jurídica entablada con la E.S.E Hospital Mental de Antioquia (incluye, entre otros, funcionarios, exfuncionarios, practicantes, aspirantes a cargos y contratistas).

PROVEEDORES Y CONTRATISTAS: El tratamiento de los datos se realizará para los fines relacionados con el desarrollo del proceso de gestión contractual de productos o servicios que la E.S.E Hospital Mental de Antioquia requiera para su funcionamiento de acuerdo con la normatividad vigente.

USUARIOS: El tratamiento de los datos personales proporcionados por los usuarios y sus familias tendrá como fin la actualización de datos del titular, caracterización y seguimiento a la población, para la gestión del riesgo en salud, utilizando la información de los servicios asistenciales. Entrega de reportes de salud pública de obligatorio cumplimiento, para dar respuesta a requerimientos a entidades de control, evaluación de indicadores de oportunidad y calidad de los servicios. Evaluación de los productos y servicios de salud ofrecidos por la institución. Y en general para cualquier otra finalidad que se derive de la naturaleza jurídica de la E.S.E Hospital Mental de Antioquia.

- El titular tiene derecho a optar por no suministrar cualquier información sensible solicitada por la E.S.E Hospital Mental de Antioquia, relacionada, entre otros, con datos sobre su origen racial o étnico, la pertenencia a sindicatos organizaciones sociales o de derechos humanos, convicciones políticas, religiosas, de la vida sexual, datos biométricos o datos de salud.
- El suministro de datos de menores de edad es facultativo y debe realizarse con autorización del padre, la madre o representante legal del menor.
- La E.S.E Hospital Mental de Antioquia vela por el uso adecuado de los datos personales de los niños, niñas y adolescentes y respetará en su tratamiento el interés superior de aquellos, asegurando la protección de sus derechos fundamentales.
- Una vez la ESE HOMO accede al dato personal se convierte en responsable y encargada del tratamiento del dato, con el deber de garantizar los derechos fundamentales del titular de la información, previstos en la Constitución Política de Colombia y en consecuencia debe:
- Conservar con las debidas seguridades la información recibida para impedir su deterioro, pérdida, alteración, uso no autorizado o fraudulento.

- Guardar reserva de la información que le sea suministrada por el titular en los términos señalados en el ordenamiento jurídico vigente aplicable a la materia.
- Utilizar los datos personales únicamente para los fines que justificaron la entrega, esto es, aquellos relacionados con la competencia funcional específica que motivó la solicitud de suministro del dato personal.
- Cumplir con las instrucciones que imparta la autoridad de control, en relación con el cumplimiento de la legislación estatutaria.

8. ATENCIÓN DE PETICIONES, CONSULTAS Y RECLAMOS

Los titulares o sus causahabientes podrán realizar peticiones relacionadas con el tratamiento de datos personales en los términos señalados en la Ley 1581 de 2012 o la norma que la modifique, adiciones o sustituya con el fin de ejercer los derechos:

- Conocer, actualizar y rectificar dichos datos;
- Ser informado sobre el uso dado a los mismos;
- Presentar consultas y reclamos;
- Revocar la autorización o solicitar la supresión de sus datos, en los casos en que sea precedente.

Para el efecto se podrán utilizar cualquiera de los siguientes canales de comunicación:

CANAL	CARACTERÍSTICAS
Presencial – Edificio	Calle 38 # 55 – 310 Bello (Ant) códig postal 051053 Horario: Lun – Jue de am a 5 pm y Viernes 7am a 3:30 pm Ventanilla de correspondencia
Línea telefónica	01 8000 41 7474
Virtual – Correo	contactenos@homo.gov.co
Virtual – Portal Web	www.homo.gov.co

9. BIBLIOGRAFÍA

- MIN TIC. (2016). Elaboración de la política general de seguridad y privacidad de la información.
- Ley Estatutaria 1581. 2012(Octubre 17). Retrieved from https://www.sisben.gov.co/Documents/Información/Leyes/LEY TRATAMIENTO DE DATOS - LEY 1581 DE 2012.pdf.
- Neira, A. L., & Spohr, J. R. (2010). Sistema de Gestión de la Seguridad de la Información. Www.Iso27000.Es, 1, 14.
- Congreso de la República de Colombia. (2014). Ley 1712 de transparencia y del derecho a la información pública nacional. Ley Del Estado.
- El congreso de Colombia. (2008). Ley Estatutaria 1266 de 2008. República de Colombia-Gobierno Nacional.