EMPRESA SOCIAL DEL ESTADO
HOSPITAL
SAN JUAN DE DIOS

# PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

# EMPRESA SOCIAL DEL ESTADO HOSPITAL SAN JUAN DE DIOS DE CONCORDIA

**Versión 2.0**

**CONCORDIA, ENERO DE 2.025**

**"MAS Y MEJORES SERVICIOS"**
**Carrera 18 N. 16-05 Concordia -Antioquia**
**Teléfono: 8446161- 844 7722**
**hospitaldeconcordia@hospital-concordia.gov.co**
**Nit. 890907297-3**

# COMITÉ DIRECTIVO.

***DOCTOR MARIO ALEJANDRO CADAVID CADAVID.***
Gerente Empresa Social del Estado.

***SEÑOR JUAN CARLOS ALVAREZ***
Subgerente Administrativo.

***SEÑOR JUAN GUILLERMO POSADA MEJÍA.***
Jefe de la Oficina de Control Interno.

***DOCTORA ANA MARIA GONZALES ESCOBAR.***
Odontóloga.

***SEÑORA JULIANA ANDREA CADAVID MESA.***
Enfermera.

***SEÑORA GLORIA MARÍA LONDOÑO GIRALDO.***
Profesional Universitaria Área Salud (Bacterióloga).

***SEÑORA CLAUDIA ORTIZ OSPINA.***
Auxiliar Administrativa (Sistema de Información y Atención al Usuario).

***SEÑORA MONICA MARIA AGUIRRE GARCIA***
Auxiliar Administrativa (Archivo Central).

***SEÑOR JORGE ESTEBAN RESTREPO VELEZ***
Técnico en Sistemas

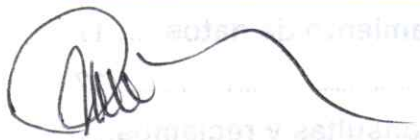
***SEÑORA LUZ ALEIDA BETANCUR***
Secretaria.

# Contenido

CUADRO DE CONTROL DE CAMBIOS ..... 4
1. Introducción. ..... 5
2. Marco Legal ..... 5
3. Definiciones ..... 9
4. Objetivo ..... 11
4.1 Objetivos Especificos ..... 11
5. Responsable ..... 11
6. Política de tratamiento de datos ..... 12
7. Estrategia De Seguridad Digital ..... 12
8. Finalidad con la que se efectúa la recolección de datos personales y tratamiento de los mismos: ..... 14
9. Deberes de la E.S.E. Hospital San Juan de Dios. ..... 16
10. Derechos de los Titulares ..... 16
11. Casos que no requieren autorización para el tratamiento de datos ..... 17
12. Entrega de información ..... 17
13. Área responsable de la atención de peticiones, consultas y reclamos. ..... 17
14. Procedimiento para la atención de peticiones, consulta y reclamos ..... 18
15. Vigencia ..... 19
16. PLAN DE IMPLEMENTACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN ..... 19

## CUADRO DE CONTROL DE CAMBIOS

| Versión | Fecha | Descripción Cambios |
|---|---|---|
| 1.0 | 2021 | Creación del documento. |
| 2.0 | 23/01/2025 | Se revisa la Versión 2.0 del Plan y se determina actualizar en alineación con el plan de desarrollo 2024-2028<br>Se actualiza los términos o definiciones<br>Se actualiza el marco legal<br>Se actualiza el objetivo general y objetivo especifico<br>Se incluye la estrategia de seguridad digital y se incluye los ejes estratégicos<br>Se actualiza el cronograma de gestión y actividades |



## 1. Introducción.

El Modelo de Seguridad y Privacidad de la Información, conduce a la preservación de la confidencialidad, integridad, disponibilidad de la información, permitiendo garantizar la privacidad de los datos.

Mediante el aprovechamiento de las TIC y el modelo de seguridad y privacidad de la información, se trabaja en el fortalecimiento de la seguridad de la información, con el fin de garantizar la protección de la misma y la privacidad de los datos de los ciudadanos y funcionarios de la entidad.

En cumplimiento de la Ley 1581 de 2012 (Art. 17 Lt. k y Art. 18 Lt. f) y del Decreto 1377 de 2013 (Art. 13.) mediante los cuales se dictan disposiciones para la protección de datos personales y en el desarrollo del derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar la información que se haya recogido sobre ellas en bases de datos o archivos, la E.S.E. Hospital San Juan de Dios en calidad de responsable del tratamiento de los datos personales de sus grupos de interés conformado por los usuarios y sus familias, colaboradores, contratistas, estudiantes, entidades responsables de pago y las entidades de inspección, vigilancia y control, información que se ha obtenido en el desarrollo de su actividad misional de prestar servicios de salud, por lo cual se compromete con el cumplimiento de la normativa mencionada y la protección de los derechos de las personas e información a su grupo de interés que adopta las siguientes políticas sobre recolección, tratamiento y uso de datos personales.

## 2. Marco Legal

- **Ley 527 de 1999**. Por la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales y se establecen las entidades de certificación y se dictan otras disposiciones.
- **Ley 594 de 2000**. Por medio de la cual se expide la Ley General de Archivos.
- Ley 850 de 2003. Por medio de la cual se reglamentan las veedurías ciudadanas
- **Ley 1266 de 2008.** Por la cual se dictan las disposiciones generales del Hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
- **Ley 1221 del 2008**. Por la cual se establecen normas para promover y regular el Teletrabajo y se dictan otras disposiciones.

- **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.
- **Ley 1341 de 2009.** Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y las comunicaciones - TIC- Se crea la agencia Nacional de espectro y se dictan otras disposiciones.
- **Ley 1437 de 2011.** Por la cual se expide el código de procedimiento administrativo y de lo contencioso administrativo.
- **Ley 1474 de 2011.** Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.
- **Ley 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.
- **Ley 1755 de 2015.** Por medio de la cual se regula el Derecho Fundamental de Petición y se sustituye un título del Código de Procedimiento Administrativo y de lo Contencioso Administrativo.
- **Ley 1915 de 2018.** Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos.
- **Ley 1952 de 2019.** Por medio de la cual se expide el código general disciplinario
- **La Ley 2294 de 2023.** Es la ley que aprueba el Plan Nacional de Desarrollo (PND) 2022-2026, denominado "Colombia Potencia Mundial de la Vida".
- **Ley 1978 de 2019.** Por la cual se moderniza el sector de las Tecnologías de la Información y las Comunicaciones TIC), se distribuyen competencias, se crea un regulador único y se dictan otras disposiciones.
- **Decreto 2609 de 2012.** Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado.
- Decreto 0884 del 2012. Por el cual se reglamenta parcialmente la Ley 1221 del 2008.
- **Decreto 1377 de 2013.** Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
- **Decreto 886 de 2014.** Por el cual se reglamenta el Registro Nacional de Bases de Datos.
- **Decreto 103 de 2015.** Por medio del cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
- **Decreto 1074 de 2015.** Por medio del cual se expide el Decreto Reglamentario del Sector Comercio, Industria y Turismo. Reglamenta parcialmente la Ley 1581 de

2012 e imparten instrucciones sobre el Registro Nacional de Bases de Datos. Artículos 25 y 26.

- **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 1080 de 2015.** Por medio del cual se expide el Decreto Reglamentario del Sector Cultura.
- **Decreto 1081 de 2015.** Por medio del cual se expide el Decreto Reglamentario del Sector Presidencia.
- **Decreto 728 de 2017.** Por el cual se adiciona el capítulo 2 al título 9 de la parte 2 del libro 2 del Decreto Único Reglamentario del sector TIC, Decreto 1078 de 2015, para fortalecer el modelo de Gobierno Digital en las entidades del orden nacional del Estado colombiano, a través de la implementación de zonas de acceso público a Internet inalámbrico
- **Decreto 1499 de 2017.** Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.
- **Decreto 1008 del 2018.** 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, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.
- **Decreto 612 de 2018:** Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado", donde se encuentra el presente Plan Estratégico de Seguridad de la Información (PESI) como uno de los requisitos a desarrollar para cumplir con esta normativa
- **Decreto 2106 de 2019.** Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública.
- **Decreto 620 de 2020.** por el cual se subroga el título 17 de la parte 2 del libro 2 del Decreto 1078 de 2015, para reglamentarse parcialmente los artículos 53, 54, 60, 61 y 64 de la Ley 1437 de 2011, los literales e), j) y literal a) del parágrafo 2 del artículo 45 de la Ley 1753 de 2015, el numeral 3 del artículo 147 de la Ley 1955 de 2019, y el artículo 9° del Decreto 2106 de 2019, estableciendo los lineamientos generales en el uso y operación de los servicios ciudadanos digitales.
- **Decreto 1064 de 2020.** Por el cual se modifica la estructura del Ministerio de Tecnologías de la Información y las Comunicaciones.
- **Decreto 338 de 2022:** Por el cual se adiciona el Titulo~1 ~a Ml\~1 2º~~ Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones".
- **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, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones"'.

- **Decreto 1263 de 2022:** "Por el cual se adiciona el Título 22 a la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de definir lineamientos y estándares aplicables a la Transformación Digital Pública".
- **Resolución 2999 del 2008.** Por el cual se adoptan las políticas de seguridad para el manejo de la información y se dictan otras normas para el uso y administración de los bienes y servicios informáticos del Ministerio TIC.
- **Resolución 2034 de 2016.** Por la cual se adoptó el Modelo de Responsabilidad Social Institucional en el Ministerio TIC.
- **Resolución 2306 de 2020.** Por la cual se actualiza el Modelo Integrado de Gestión (MIG) del Ministerio/Fondo de Tecnologías de la Información y las Comunicaciones y se deroga la Resolución 911 de 2018
- **Resolución 1151 de 2019**. Por la cual se establecen las condiciones especiales del Teletrabajo en el Ministerio de Tecnologías de la Información y las Comunicaciones, y se deroga la Resolución 0002133 del 3 de agosto de 2018
- **Resolución 924 de 2020.** Por la cual se actualiza la política de tratamiento de datos personales del Ministerio/Fondo Único de TIC y se deroga la resolución 2007 de 2018.
- **Resolución 2256 de 2020.** Por la cual se actualiza la Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de los servicios del Ministerio/Fondo de Tecnologías de la Información y las Comunicaciones y se definen lineamientos frente al uso y manejo de la información y se deroga la resolución 1124 de 2020.
- **Resolución 1519 de 2020:** Estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos.
- **Resolución 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 como habilitador de la política de Gobierno Digital". Manual de Gobierno Digital – MINTIC.
- **Resolución 460 de 2022:** Por la Cual Se expide el Plan Nacional de Infraestructura de Datos y su hoja de ruta en el desarrollo de la Política de Gobierno Digital, y se dictan los lineamientos generales para su implementación.
- **Resolución 746 de 2022:** Por la cual se fortalece el modelo de seguridad y privacidad de la información y se definen lineamientos adicionales a los establecidos en la resolución 500 de 2021.
- **Directiva presidencial 02 de 2022:** Reiteración de la Política Publica en Materia de Seguridad Digital.

- **CONPES 3701 de 2011.** Lineamientos de Política para Ciberseguridad y Ciberdefensa.
- **CONPES 3854 de 2016.** Política Nacional de Seguridad digital.
- **Conpes 3975 de 2019:** Política Nacional para la Transformación Digital e Inteligencia Artificial.
- **CONPES 3995 de 2020.** Política Nacional de Confianza y Seguridad Digital.
- **Directiva presidencial 003 de 2021:** Lineamientos para el uso de servicios en la nube, inteligencia artificial, seguridad digital y gestión de datos.

## 3. Definiciones

Para efectos de la ejecución de la presente política y de conformidad con la normatividad legal, serán aplicables las siguientes definiciones:

- **Autorización:** Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales.

- **Base de Datos:** Conjunto organizado de datos personales que sea objeto de Tratamiento.

- **Confidencialidad:** Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

- **Dato personal:** Cualquier información vinculada o que pueda asociarse a una o a varias personas naturales determinadas o determinables.

- **Dato personal semiprivado:** Son aquellos datos que no tienen una naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no solo a su titular, sino, a un grupo de personas o a la sociedad en general.

  En este caso, para su tratamiento se requiere la autorización expresa del Titular de la información. Por ejemplo: datos de carácter financiero, datos relativos a las relaciones con las entidades de seguridad social (EPS, AFP, ARL, Cajas de Compensación).

- **Dato personal sensible:** Son 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.

- **Dato personal privado:** Es un dato personal que por su naturaleza íntima o reservada solo interesa a su Titular y para su tratamiento requiere de su autorización expresa. Por ejemplo: Nivel de escolaridad, libros de los comerciantes, entre otros.

- **Dato personal público:** Es aquel tipo de dato personal que las normas y la Constitución han determinado expresamente como públicos y, para cuya recolección y tratamiento, no es necesaria la autorización del Titular de la información. Por ejemplo: estado civil de las personas, datos contenidos del RUNT, datos contenidos en sentencias judiciales ejecutoriadas, entre otros.

- **Disponibilidad:** Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

- **Encargado del Tratamiento:** 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.

- **Gestión de Riesgo:** Proceso de identificación y evaluación de riesgos y la toma de acciones efectivas para reducirlos a un nivel aceptable. Incluye la valoración de riesgos; análisis costo beneficio de las acciones y controles de mitigación, y la selección, implementación y valoración de controles de seguridad.

- **Incidente digital:** Evento intencionado o no intencionado que puede cambiar el curso esperado de una actividad en el medio digital y que genera impactos sobre los objetivos. (CONPES 3854, pág. 87).

- **Incidente de seguridad de la información:** Uno o múltiples eventos de seguridad de la información relacionados e identificados que pueden dañar los activos de información de la organización o comprometer sus operaciones. (ISO/IEC 27035:2016).

- **Información:** Es todo aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración.

- **Ingeniería social:** Consiste en la manipulación de las personas para que voluntariamente realicen actos que normalmente no harían.

- **Integridad:** Propiedad de la información relativa a su exactitud y completitud.
- **MSPI:** Modelo de Seguridad y Privacidad de la Información.
- **Responsable del Tratamiento:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos.
- **SGSI:** Sigla del Sistema de Gestión de la Seguridad de la Información. (ISMS en inglés, Information Security Management System).
- **Titular:** Persona natural cuyos datos personales sean objeto de Tratamiento.
- **Tratamiento:** Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

## 4. Objetivo

Generar un documento de lineamientos de buenas prácticas en Seguridad y Privacidad para la ESE. Con el propósito de identificar el nivel implementación del Modelo de Seguridad y Privacidad de la Información en la entidad, se toma como referencia el Instrumento de Evaluación del MSPI que es una herramienta creada por el Ministerio de Tecnologías y las Comunicaciones MINTIC.

### 4.1 Objetivos Especificos

- Promover el uso de mejores prácticas de seguridad de la información, para ser la base de aplicación del concepto de Seguridad Digital.
- Revisar los roles relacionados con la privacidad y seguridad de la información al interior de la entidad para optimizar su articulación.
- Evaluar en el ciclo PHVA los componentes de planificación, implementación, evaluación de desempeño y mejora continua del Modelo de Seguridad y Privacidad de la Información (MSPI), teniendo como referencia el ítem de prueba conocidos como requisitos de cumplimiento.

## 5. Responsable

- Líderes de Procesos
- Todos los usuarios o funcionarios de la institución.

## 6. Política de tratamiento de datos

La E.S.E. Hospital San Juan de Dios de Concordia - Antioquia, está comprometida en dar un correcto uso y tratamiento de los datos personales y datos personales sensibles de sus titulares, evitando el acceso no autorizado a terceros que permita conocer, vulnerar, modificar, divulgar y/o destruir la información, para lo cual cuenta con políticas de seguridad de la información que incluyen medidas de control de obligatorio cumplimiento.

La Entidad, solicita a los titulares de la información los datos necesarios para prestar los servicios de salud cumpliendo con las funciones asignadas por la normativa vigente. La información sensible requerida será de libre y voluntaria entrega por parte del respectivo Titular.

Salvo las excepciones previstas en la ley, el tratamiento de los datos personales sólo podrá realizarse con el consentimiento previo, expreso e informado de sus titulares manifestado de forma oral o mediante conductas inequívocas del Titular que permitan concluir de forma razonable que otorgó la autorización.

La E.S.E. Hospital San Juan de Dios, solicitará a las entidades responsables de pago, colaboradores, estudiantes y contratistas, los datos personales necesarios para establecer la respectiva relación y/o vinculación (civil, laboral, comercial o educativa). La información sensible requerida será de libre y voluntaria entrega por parte del respectivo Titular, quien deberá otorgar su consentimiento y autorización para su respectivo tratamiento.

## 7. Estrategia De Seguridad Digital

La E.S.E. Hospital San Juan de Dios de Concordia - Antioquia establecerá una estrategia de seguridad digital en la que se integren los principios, políticas, procedimientos, guías, manuales, formatos y lineamientos para la gestión de la seguridad de la información, teniendo como premisa que dicha estrategia gira entorno a la implementación del Modelo de Seguridad y Privacidad de la Información -MSPI, así como de la guía de gestión de riesgos de seguridad de la información y del procedimiento de gestión de incidentes. Por tal motivo, La E.S.E. define las siguientes 5 estrategias específicas:

1) Liderazgo de seguridad de la información
2) Gestión de riesgos
3) Implementación de controles
4) Gestión de incidentes
5) Concientización

Estrategia De Seguridad Digital

A continuación, se describe el objetivo de cada una de las estrategias específicas a implementar, alineando las actividades a lo descrito dentro del MPSI y la Resolución 500 de 2021:

| ESTRATEGIA / EJE | DESCRIPCIÓN/OBJETIVO |
|---|---|
| **Liderazgo de seguridad de la información** | Asegurar que se establezca el Modelo de Seguridad y Privacidad de la Información (MSPI) a través de la aprobación de la política general y demás lineamientos que se definan buscando proteger la confidencialidad, integridad y disponibilidad de la información teniendo como pilar fundamental el compromiso de la alta dirección y de los líderes de las diferentes dependencias y/o procesos de la Entidad a través del establecimiento de los roles y responsabilidades en seguridad de la información. |
| **Gestión de riesgos** | Determinar los riesgos de seguridad de la información a través de la planificación y valoración que se defina buscando prevenir o reducir los efectos indeseados tendiendo como pilar fundamental la implementación de controles de seguridad para el tratamiento de los riesgos. |
| **Concientización** | Fortalecer la construcción de la cultura organizacional con base en la seguridad de la información para que convierta en un hábito, promoviendo las políticas, procedimientos, normas, buenas prácticas y demás lineamientos, la transferencia de conocimiento, la asignación y divulgación de responsabilidades de todo el personal de la entidad en seguridad y privacidad de la información. |
| **Implementación de controles** | Planificar e implementar las acciones necesarias para lograr los objetivos de seguridad y privacidad de la información y mantener la confianza en la ejecución de los procesos de la Entidad, se pueden subdividir en controles tecnológicos y/o administrativos. |
| **Gestión de incidentes** | Garantizar una administración de incidentes de seguridad de la información con base a un enfoque de integración, análisis, comunicación de los eventos e incidentes y las debilidades de seguridad en pro de conocerlos y resolverlos para minimizar el impacto negativo de estos en la Entidad. |

## 8. Finalidad con la que se efectúa la recolección de datos personales y tratamiento de los mismos:

El tratamiento de los datos personales proporcionados por los usuarios y sus familias tendrá la siguiente finalidad:

- Para la prestación de los servicios asistenciales de sus usuarios y familias.
- Actualización de datos entregados por el Titular.
- Caracterización de la población atendida basada en RIPS
- Entrega de reportes de Salud Pública de obligatorio cumplimiento.

- Dar respuesta a requerimientos a entidades de control.
- Evaluación de indicadores de oportunidad y calidad de los servicios.
- Ejercer acciones legales y en la defensa de las mismas.
- Suministro de información a las autoridades competentes en caso de ser requerida.
- En general para cualquier otra finalidad que se derive de la naturaleza jurídica de la E.S.E. Hospital San Juan de Dios.

El tratamiento de los datos personales proporcionados por los colaboradores tendrá la siguiente finalidad:

- Establecer una relación contractual.
- Evaluaciones de desempeño, satisfacción laboral, crecimiento personal, bienestar, seguridad y salud en el trabajo.
- Cumplir el proceso de afiliación al Sistema General de Seguridad Social Integral (Entidades Promotoras de Salud, Administradoras de riesgos laborales, Fondos de pensiones y cesantías, Caja de Compensación)
- Efectuar el proceso de Remuneración.
- Ejercer acciones legales y en la defensa de las mismas.
- Cumplir con exigencias judiciales.
- Suministro de información a las autoridades competentes en caso de ser requerida.
- En general para cualquier otra finalidad que se derive de la vinculación contractual.

El tratamiento de los datos personales proporcionados por las entidades responsables de pago y contratistas, sean personas naturales o jurídicas, tendrá la siguiente finalidad:

- Realizar la vinculación contractual.
- Efectuar el reconocimiento económico por la prestación del servicio.
- Suministro de información a las autoridades competentes en caso de ser requerida.
- Ejercer acciones legales y en la defensa de las mismas.
- Cumplir con exigencias judiciales.

## 9. Deberes de la E.S.E. Hospital San Juan de Dios.

- Garantizar al usuario el pleno y efectivo derecho constitucional de habeas data.
- Mantener la información en condiciones de seguridad y privacidad.
- Hacer uso de la información para los fines misionales y previstos en la ley.
- Tramitar de manera oportuna los reclamos que tengan los usuarios frente a la información consignada en la base de datos.
- No vender, circular o intercambiar la base de datos de sus usuarios, sin causa legal o contractual que lo justifique.

## 10. Derechos de los Titulares

El Titular de los datos personales y datos personales sensibles tendrá los siguientes derechos:

- Conocer, actualizar y rectificar los datos que aparezcan en la misma. Este derecho se podrá ejercer, entre otros frente a datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo tratamiento esté expresamente prohibido o no haya sido autorizado.
- Conocer por qué y para qué la E.S.E. Hospital San Juan de Dios, recolecta información en base de datos.
- Revocar en cualquier momento la autorización dada para contener información personal en las bases de datos de la institución.
- Revocar la autorización y/o solicitar la supresión del dato cuando en el tratamiento considere que no se respetan los principios, derechos y garantías constitucionales y legales. La revocatoria y/o supresión procederá cuando la Superintendencia de Industria y Comercio haya determinado que en el tratamiento el responsable o encargado han incurrido en conductas contrarias a esta ley y a la constitución.
- Poner queja ante la Superintendencia de Industria y Comercio, cuando considere que le ha sido violado por parte de la institución su derecho al Habeas Data.
- Derecho a solicitar prueba de la autorización: salvo en los eventos en los cuales, según las normas legales vigentes, no se requiera de la autorización para realizar el tratamiento.

## 11. Casos que no requieren autorización para el tratamiento de datos

La autorización del Titular no será necesaria cuando se trate de:

- Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial.
- Datos de naturaleza pública.
- Casos de urgencia médica o sanitaria.
- Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos.
- Datos relacionados con el Registro Civil de las Personas.

## 12. Entrega de información

La información que reúna las condiciones establecidas en el Art. 13 de la Ley 1581 de 2012, podrá suministrarse a las siguientes personas:

- A los Titulares, sus causahabientes o sus representantes legales.
- A las entidades públicas o administrativas en ejercicio de sus funciones legales o por orden judicial.
- A los terceros autorizados por el Titular o por la ley.

## 13. Área responsablede la atención de peticiones, consultas y reclamos.

Se deberá dar trámite a lo estipulado en la Ley 1755 de 2015. Por medio de la cual se regula el Derecho Fundamental de Petición y se sustituye un título del Código de Procedimiento Administrativo y de lo Contencioso Administrativo o la norma que la modifique o sustituya

El área responsable de la atención de peticiones, consultas y reclamos será SIAU de la E.S.E. Hospital San Juan de Dios", la cual una vez reciba la solicitud de acuerdo con el capítulo siguiente la remitirá al área responsable del tratamiento de los datos.

## 14. Procedimiento para la atención de peticiones, consulta y reclamos

- El Titular de la información contenida en la base de datos de la E.S.E. Hospital San Juan de Dios o por su representante legal, podrá ejercer su derecho de conocer, actualizar, rectificar, suprimir y revocar la información contenida en las mismas, mediante los correos electrónicos siau@hospital-concordia.gov.co, contacto@hospital-concordia.gov.co y en comunicación escrita a la dirección Carrera 18 N. 16-05

- La solicitud debe ser clara en lo que se pretende, ya sea conocer, actualizar, rectificar, suprimir y/o revocar la información que se encuentra contenida en una base de datos. Además, deberá contener los datos de contacto del peticionario para poder darle una respuesta.

- Independientemente del mecanismo utilizado para la radicación de solicitudes de consulta, las mismas serán atendidas en un término máximo de diez (10) días hábiles contados a partir de la fecha de su recibo. Cuando no fuere posible atender la consulta dentro de dicho término, se informará al interesado, expresando los motivos de la demora y señalando la fecha en que se atenderá su consulta, la cual en ningún caso podrá superar los cinco (5) días hábiles siguientes al vencimiento del primer término.

- Los reclamos para corrección, actualización o supresión de datos serán contestados dentro de los quince (15) días hábiles siguientes, contados a partir del día siguiente a la fecha de su recibo. Cuando no fuere posible atenderlo dentro de dicho término se informará al interesado antes del vencimiento del referido plazo los motivos de la demora y la fecha en que se atenderá su reclamo, la cual en ningún caso podrá superar los ocho (8) días hábiles siguientes al vencimiento del primer término.

- Si el reclamo resulta incompleto, se requerirá al interesado dentro de los cinco (5) días siguientes a la recepción del reclamo para que subsane las fallas. Una vez recibido el reclamo completo, se incluirá en la base de datos una leyenda que diga "reclamo en trámite" y el motivo del mismo, en un término no mayor a dos (2) días hábiles. Dicha leyenda deberá mantenerse hasta que el reclamo sea decidido.

- De igual forma, si Transcurridos dos (2) meses desde la fecha del requerimiento, sin que el solicitante presente la información requerida, se entenderá que ha desistido del reclamo.

- La primera instancia de la reclamación será la E.S.E. Hospital San Juan de Dios, y una vez agotada esta sin respuesta satisfactoria, podrá el Titular recurrir a la Superintendencia de Industria y Comercio.

## 15. Vigencia

La presente política rige a partir de la fecha de su publicación y su vigencia estará supeditada a la finalidad del tratamiento de los datos personales propios de la naturaleza jurídica de la E.S.E. Hospital. Antonio Roldán.

## 16. Plan De Implementación Del Modelo De Seguridad Y Privacidad De La Información

El Plan de implementación para la dimensión de Seguridad y Privacidad de la Información comprende el siguiente cronograma y se le hace seguimiento mes a mes.

| GESTIÓN | ACTIVIDADES | TAREA | RESPONSABLE TAREA | FECHAS DE PROGRAMACIÓN | |
|---|---|---|---|---|---|
| | | | | INICIO | FINAL |
| Activos de Información | Definir lineamientos para el levantamiento de activos de información | Actualización de metodología e instrumento de levantamiento de activos de información | Equipo de activos | Junio - 2025 | Julio – 2025 |
| | Levantamiento Activos de Información | Socializar la guía de activos de Información. | Equipo de activos | Junio - 2025 | Julio – 2025 |
| | | Validar activos de información en el instrumento | Líder del proceso y equipo de activos | Julio - 2025 | Agosto – 2025 |
| | | Identificar nuevos activos de información en cada dependencia | Líder del proceso y equipo de activos | Julio - 2025 | Agosto – 2025 |
| | | Revisar los instrumentos de activos de Información y realimentar a las áreas con las modificaciones. | Equipo de activos | Agosto - 2025 | Septiembre – 2025 |
| | | Realizar correcciones a los instrumentos de activos de Información, Cambios físicos de la ubicación de activos de información | Líder del proceso y equipo de activos | Agosto - 2025 | Septiembre – 2025 |

| GESTIÓN | ACTIVIDADES | TAREA | RESPONSABLE TAREA | FECHAS DE PROGRAMACIÓN | |
|---|---|---|---|---|---|
| | | | | INICIO | FINAL |
| | | Realizar informe de actualización a los activos de información por alguna de las siguientes novedades: Actualizaciones al proceso al que pertenece el activo, Adición de actividades al proceso, Inclusión de un nuevo activo, Cambios o migraciones de sistemas de información en donde se almacenan o reposan activos de la ubicación ya inventariados, Materialización de riesgos que cambien la criticidad del activo. | Líder del proceso y equipo de activos | Septiembre - 2025 | Diciembre - 2025 |
| | Publicación de Activos de Información | Validar y aceptar los activos de información para su publicación, por cada líder de proceso. | Líder del proceso y equipo de activos | Septiembre - 2025 | Octubre – 2025 |
| | | Consolidar el instrumento de activos de Información. | Equipo de activos | Octubre - 2025 | Noviembre – 2025 |
| | Registros activos de información ley 1712 | Publicar los instrumentos de activos de información consolidado | Equipo de activos | Diciembre - 2025 | Diciembre - 2025 |
| | | Actualizar el instrumento de Registro Activos de Información con el insumo de los instrumentos de activos de Información. | Equipo de Activos, Líder Asesora Jurídica. | Octubre - 2025 | Octubre – 2025 |
| | | Enviar a control de legalidad el instrumento de Registro Activos de información. | Líder Asesora Jurídica | Noviembre - 2025 | Noviembre – 2025 |
| | | Publicación del Registro Activos de Información en el sitio web de la Entidad. | Equipo de activos | Diciembre - 2025 | Diciembre - 2025 |
| | Reporte Datos Personales | Reportar líder de Datos personales o Seguridad de la Información la información recolectada en el instrumento de activos de información, correspondiente a bases de datos. | Equipo de activos | Septiembre - 2025 | Septiembre – 2025 |
| Gestión de riesgo | Actualización de lineamientos de riesgos | Actualizar política y metodología de gestión de riesgos | Equipo de Gestión de Riesgos | Marzo - 2025 | Agosto – 2025 |
| | Sensibilización | Socialización Guía y Herramienta - Gestión de Riesgos de Seguridad y privacidad de la Información, Seguridad Digital y Continuidad de la Operación | Equipo de Gestión de Riesgos | Abril - 2025 | Mayo – 2025 |

| GESTIÓN | ACTIVIDADES | TAREA | RESPONSABLE TAREA | FECHAS DE PROGRAMACIÓN | |
|---|---|---|---|---|---|
| | | | | INICIO | FINAL |
| | Identificación de Riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y continuidad de la Operación | Identificación, Análisis y Evaluación de Riesgos - Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación | Equipo de Gestión de Riesgos | Mayo - 2025 | Mayo – 2025 |
| | | Realimentación, revisión y verificación de los riesgos identificados (Ajustes) | Equipo de Gestión de Riesgos | Septiembre - 2025 | Septiembre – 2025 |
| | Aceptación de Riesgos Identificados | Aceptación, aprobación Riesgos identificados y planes de tratamiento | Equipo de Gestión de Riesgos | Junio - 2025 | Noviembre – 2025 |
| | Publicación | Publicación Matriz de riesgos | Equipo de Gestión de Riesgos | Junio - 2025 | Noviembre – 2025 |
| | Seguimiento Fase de Tratamiento | Seguimiento Estado planes de tratamiento de riesgos identificados y verificación de evidencias | Equipo de Gestión de Riesgos | Junio - 2025 | Diciembre - 2025 |
| | Evaluación de riesgos residuales | Evaluación de riesgos residuales | Equipo de Gestión de Riesgos | Junio - 2025 | Diciembre - 2025 |
| | Mejoramiento | Identificación de oportunidades de mejora acorde a los resultados obtenidos durante la evaluación de riesgos residuales | Equipo de Gestión de Riesgos | Junio - 2025 | Diciembre - 2025 |
| | | Actualización Guía Gestión de Riesgos Seguridad de la información, de acuerdo con los cambios solicitados. | Equipo de Gestión de Riesgos | Junio - 2025 | Diciembre - 2025 |
| | Monitoreo y Revisión | Generación, presentación y reporte de indicadores | Equipo de Gestión de Riesgos | Junio - 2025 | Diciembre - 2025 |
| **Gestión de Incidentes de Seguridad de la Información** | Publicar y Socializar el procedimiento actualizado de incidentes de seguridad de la información | Revisión, actualización y publicación del procedimiento de incidentes de seguridad de la información. | Encargado de la Gestión de Incidentes de Seguridad de la Información. | Febrero - 2025 | Marzo – 2025 |
| | | Socializar el procedimiento a los, indicando los cambios en el procedimiento | Encargado de la Gestión de Incidentes de Seguridad de la Información. | Febrero - 2025 | Marzo – 2025 |
| | | Socializar el procedimiento a los soportes en sitio y Mesa de Servicios, indicando los cambios en el procedimiento | Encargado de la Gestión de Incidentes de Seguridad de la Información. | Febrero - 2025 | Marzo – 2025 |
| | | Socializar el procedimiento a los colabores de la Entidad. | Equipo de Gestión de Riesgos | Febrero - 2025 | Marzo – 2025 |

| GESTIÓN | ACTIVIDADES | TAREA | RESPONSABLE TAREA | FECHAS DE PROGRAMACIÓN | |
|---|---|---|---|---|---|
| | | | | INICIO | FINAL |
| | Gestionar los incidentes de Seguridad de la Información identificados<br>Eventos / vulnerabilidades | Gestionar los incidentes de seguridad de la información de acuerdo con lo establecido en el procedimiento definido. | Lideres de proceso y responsables asignados | Febrero - 2025 | Marzo – 2025 |
| | | Realizar seguimiento a los informes de eventos y vulnerabilidades | Equipo de Gestión de Riesgos | Febrero - 2025 | Marzo – 2025 |
| Concientización | Concientizar a todo el personal de la institución de la importancia de la implementación de la Política de Seguridad y Privacidad de la Información. | Realizar Plan de sensibilización anual. | Líder del proceso | Marzo de 2025 | Diciembre - 2025 |
| | | Realizar jornadas de sensibilización a todo el personal de la entidad | Líder del proceso | Marzo de 2025 | Diciembre - 2025 |
| | | Realizar trasferencia de conocimiento a colaboradores de la Entidad a través de cursos especializado en seguridad y privacidad de la información. | Líder del proceso | Marzo de 2025 | Diciembre - 2025 |
| | | Medir el grado de señsibilización a toda la Entidad. | Líder del proceso | Marzo de 2025 | Diciembre - 2025 |

**MARIO ALEJANDRO CADAVID CADAVID.**
**Gerente de la Empresa Social del Estado.**