



# Política General de Seguridad y Privacidad de la Información



Elaborar la política general de seguridad y privacidad de la información, por parte del ESEHMRS con el compromiso de implementar, mantener y mejorar la seguridad y privacidad de la información para garantizar la confidencialidad, integridad y disponibilidad de la información del Hospital Mental Rudesindo Soto.

La política de seguridad y privacidad de la información aplica a todos los procesos que manejan información de la Entidad y debe ser aplicada por todos los servidores públicos, contratistas de prestación de servicios, proveedores, terceros que tengan acceso a la información y al sistema.

## Política Seguridad y privacidad de la información - ESEHMRS

### Proceso Gestión de Sistemas de Información y Tecnología

Descripción	Objetivo
El control de la información de la Política de Gestión del Riesgo, y se definen los parámetros internos y externos (to the Entity), que se refieren en cuenta para la gestión de riesgo.	Contexto
El control de la información de la Política de Gestión del Riesgo, y se definen los parámetros internos y externos (to the Entity), que se refieren en cuenta para la gestión de riesgo.	Confidencialidad
El control de la información de la Política de Gestión del Riesgo, y se definen los parámetros internos y externos (to the Entity), que se refieren en cuenta para la gestión de riesgo.	Acceso de la información

# Política General de Seguridad y Privacidad de la Información

## 1. OBJETIVO

Establecer la política general de seguridad y privacidad de la información, por parte del ESEHMRS con el compromiso de implementar, mantener y mejorar la seguridad y privacidad de la información, para garantizar la confidencialidad, integridad y disponibilidad de la información del Hospital Mental Rudesindo Soto.



## 2. ALCANCE

La política de seguridad y privacidad de la información, aplica a todos los procesos que manejen información de la Entidad y debe ser aplicada por todos los servidores públicos, contratistas de prestación de servicios, proveedores y terceros que tengan acceso a la información del Instituto.

## 3. DEFINICIONES

<u>TÉRMINO</u>	<u>DEFINICIÓN</u>
Activos de información	Cualquier recurso (físico lógico o intangible), de la organización que pueda procesar, contener o ayudar a proteger la información y que tenga valor para ella.
Confidencialidad	Propiedad de la información, de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.
Contexto	El contexto, es decir, la situación, el ambiente o el entorno, se utiliza para la definición de la Política de gestión del Riesgo. <sup>1</sup> Y se definen los parámetros internos y externos (de la Entidad), que se tendrán en cuenta para la gestión del riesgo.

<sup>1</sup> [Tomado de la norma NTC-ISO 31000. 2. Términos y definiciones 2.9 Establecimiento del contexto.]

# Política General de Seguridad y Privacidad de la Información



Continuidad del Negocio	Describe los procesos y procedimientos que una organización pone en marcha, para garantizar, que las funciones esenciales puedan continuar durante y después de un desastre.
Disponibilidad	Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.
Información	Datos organizados de tal forma que tienen un significado.
Integridad	Propiedad de la información relativa a su exactitud y completitud.
Monitoreo	Mesa de trabajo anual, la cual tiene como finalidad revisar, informar, actualizar o redefinir los riesgos de seguridad de la información, en cada uno de los procesos, partiendo del resultado de los seguimientos y/o hallazgos de los entes de control o las diferentes auditorías de los sistemas integrados de gestión.
Recursos Tecnológicos	Elementos de tecnología, que pueden ser hardware y/o software, tales como equipos de cómputo, servidores, impresoras, teléfonos, faxes, programas y/o aplicativos de software, sistemas de información, entre otros.
Tecnología de la Información	Hace referencia a las aplicaciones, información e infraestructura requerida por una entidad para apoyar el funcionamiento de los procesos y estrategia de negocio.

## 4. NORMATIVIDAD

**Ley 23 de 1982.** Ley sobre derechos de autor.

**Ley 527 de 1999.** Por medio de 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 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 1955 de 2019.** Por la cual se expide el Plan Nacional de Desarrollo, 2018-2022.

**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.



## Política General de Seguridad y Privacidad de la Información

**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 767 de 16 de mayo de 2022.** Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y de subrogo el Capítulo 1 del Título 9 de la Parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único del Sector de Tecnologías de la información y las Comunicaciones.

**Resolución Distrital 305 de 2008.** Por la cual se expiden políticas públicas, para las entidades, organismos y órganos de control del Distrito Capital, en materia de Tecnologías de la Información y Comunicaciones, respecto a la planeación, seguridad, democratización, caridad, racionalización del gasto, conectividad, infraestructura de Datos Espaciales y Software Libre.

**Resolución 004 de 2017.** Por la cual se modifica la Resolución 305 de 2008 de la CDS.

**Resolución 500 de 2021 MINTIC.** 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 habilitados de la política de gobierno digital

**Documento CONPES 3701 de 2011 -** Lineamientos de Políticas sobre ciberseguridad y ciberdefensa.

**Documento CONPES 3854 de 2016 -** Política Nacional de Seguridad Digital.

**Documento CONPES 3995 de 2020 -** Política Nacional De Confianza y Seguridad Digital

**NTC/ISO 27001:2013.** Sistemas de la Información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos.

**2021 RESOLUCIÓN 331 -31 DICIEMBRE 2021** por medio del cual se adoptan las políticas de gestión y las 17 políticas de MIPG para la ESE Hospital Mental Rudesindo Soto y se dictan otras disposiciones.

### 5. POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El Hospital Mental Rudesindo Soto se compromete a implementar, mantener y mejorar la seguridad y privacidad de la información, mediante una adecuada gestión de los activos de información, riesgos e incidentes de seguridad de la información; con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de la información y los datos.

La presente política se encuentra alineada al propósito de la Entidad y apoya el cumplimiento de los objetivos estratégicos:

1. Fomentar la apropiación social del patrimonio cultural tangible e intangible.
2. Gestionar la recuperación de Bienes y Sectores de Interés Cultural en el Distrito Capital.
3. Promover la inversión pública y privada con el fin de garantizar la sostenibilidad del patrimonio cultural.

# Política General de Seguridad y Privacidad de la Información

4. Divulgar los valores de patrimonio cultural en todo el Distrito Capital.
5. Fortalecer la gestión y administración institucional.

## 5.1 **Objetivos del Modelo de Seguridad y Privacidad de la Información** MSPI

El Hospital Mental Rudesindo Soto en su propósito de dar cumplimiento a la política de seguridad y privacidad de la información establece los siguientes objetivos:

1. Identificar y valorar los activos de información del Hospital Mental Rudesindo Soto.
2. Gestionar de manera eficaz los riesgos de seguridad y privacidad de la información identificada en la Entidad.
3. Sensibilizar a los colaboradores, contratistas y terceros que tengan acceso a la información del Hospital Mental Rudesindo Soto., sobre el manejo seguro de la información institucional.
4. Cumplir con los criterios y requisitos de seguridad atendiendo el marco normativo y legal de la entidad.

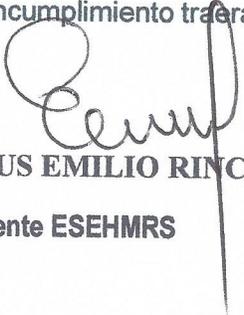
## 5.2 **Alcance/Aplicabilidad**

Esta política aplica a todos servidores públicos, contratistas y terceros que tengan acceso a la información del Hospital Mental Rudesindo Soto., en particular a los procesos misionales, gestión documental y gestión de sistemas de información y tecnología.

## 5.3 **Nivel de cumplimiento**

Todas las personas cubiertas por el alcance y aplicabilidad deberán dar cumplimiento a la presente política.

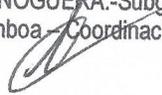
Su incumplimiento traerá consigo, las consecuencias legales correspondientes.



**JESUS EMILIO RINCON VERA**

**Gerente ESEHMRS**

Reviso: MIGUEL ALEXANDER NOGUERA.-Subgerente Administrativo en función de jefe de  
Reviso: Sonia Rocío Flórez Gamboa.-Coordinación de planeación institucional.



talento humano