	HOSPITAL REGIONAL DE MONIQUIRA E.S.E		
	FORMATO PLAN		
	PROCESO DE GESTIÓN DE TECNOLOGÍA		
	SUBPROCESO: SISTEMAS		
CÓDIGO:	GT-PL-02	VERSIÓN	V1-2023


PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN



Calle 4 A N° 9-101 Barrio Ricaurte – Teléfono (8) 7282630 -7281746 -7282854


Correo electrónico: contactenos@hrm.gov.co Página WEB: www.hrm.gov.co

NOMBRE		CARGO	FECHA
ELABORÓ	Eduardo Mateus Camacho	Líder de Sistemas	01/2023
VALIDÓ	Diego Fernando Rivera Castro	Jefe de la Oficina Asesora de Planeación	01/2023
APROBÓ	Comité Institucional de Gestión y Desempeño		01/2023

	HOSPITAL REGIONAL DE MONIQUIRA E.S.E		
	FORMATO PLAN		
	PROCESO DE GESTIÓN DE TECNOLOGÍA		
	SUBPROCESO: SISTEMAS		
CÓDIGO:	GT-PL-02	VERSIÓN	V1-2023

CONTENIDO

1. Introducción.....	3
2. Objetivo del Plan.....	4
3. Objetivos Específicos.....	4
4. Alcance del Documento.....	5
5. Definiciones.....	5
6. Marco Normativo.....	8
7. Descripción Del Plan.....	10
8. Acciones de Mejoramiento.....	10
9. Barrera de mejoramiento y control propuesto.....	10
10. Fase Diagnostico.....	11
11. Fase Planificación.....	11
12. Cronograma.....	13
13. Mapa de riesgos en la prestación de servicios.....	¡Error! Marcador no definido.
CONTROL DE CAMBIOS.....	14

	HOSPITAL REGIONAL DE MONIQUIRA E.S.E		
	FORMATO PLAN		
	PROCESO DE GESTIÓN DE TECNOLOGÍA SUBPROCESO: SISTEMAS		
	CÓDIGO:	GT-PL-02	VERSIÓN

1. INTRODUCCIÓN

El Plan de Seguridad y Privacidad de la Información, tiene como finalidad la implementación en el Hospital Regional de Moniquirá ESE. las mejoras prácticas dadas por el Departamento de Administrativo de la Función Pública con su estrategia MIPG y el Ministerio de las Tecnologías e Información en el diagnóstico, planificación, implementación, gestión y mejoramiento continuo, del Modelo de Seguridad y Privacidad de la Información, teniendo en cuenta que el objetivo principal del área de sistemas es brindar a los usuarios recursos informáticos con la calidad y la cantidad que demanden, es decir, prestando servicios con continuidad los 365 días del año de manera confiable.


Siendo conscientes de que la cantidad de recursos de cómputo y de telecomunicaciones con que cuenta el hospital son de consideración y se requiere que se protejan para garantizar su buen funcionamiento.

Este plan será aplicado a los clientes internos, externos y partes interesadas en la gestión adecuada de la seguridad de la información, la gestión de activos, la gestión de riesgos y la continuidad en la prestación de los servicios ofrecidos.

Dichos requisitos y lineamientos serán aplicados a los procesos estratégicos, misionales y de apoyo en el hospital, por tal motivo, deberán ser conocidos y cumplidos por todo el recurso humano (servidores, proveedores y terceros), que accedan a los sistemas de información e instalaciones físicas del hospital.

Este se elabora con base al Modelo de Seguridad y Privacidad de la Información emitida por MinTIC con el fin de dar a conocer cómo se realizará la implementación y socialización del componente de Gobierno en línea en el Eje Temática de la Estrategia en Seguridad y Privacidad de la Información, el Comprende las acciones transversales, tendientes a proteger la información y los sistemas de información, de acceso, uso, divulgación, interrupción o destrucción no autorizada, salvaguardando los datos y asistenciales y administrativos en nuestro hospital, garantizando la Confidencialidad, Integridad y Disponibilidad de la información, con instrumentos que permitan la autenticación y no repudio en sus procesos informáticos.

El Hospital Regional de Moniquirá ESE., se enfocará en el Modelo de Seguridad y Privacidad de la Información –MSPI-, en cuanto a la Gestión de Riesgos será utilizada la metodología “Guía de Riesgos” del Departamento Administrativo de la Función Pública teniendo en cuenta como referente la Norma ISO 31000 con el

	HOSPITAL REGIONAL DE MONQUIRÁ E.S.E		
	FORMATO PLAN		
	PROCESO DE GESTIÓN DE TECNOLOGÍA SUBPROCESO: SISTEMAS		
	CÓDIGO:	GT-PL-02	VERSIÓN

objetivo de generar buenas prácticas de gobierno corporativo y del mejoramiento continuo en la gestión de riesgos.


Este plan se debe actualizar de forma periódica (anual) garantizando que se encuentre acorde a los objetivos estratégicos organizacionales.

2. OBJETIVO DEL PLAN

El Plan de Seguridad y Privacidad de la Información, tiene como propósito plantear las diferentes actividades a realizar con el fin de identificar los activos y riesgos de información asociados a los diferentes procesos que el Hospital Regional de Monquirá ESE. posee dentro del modelo organización, de tal manera que se puedan medir los riesgos inherentes y residuales de la entidad

3. OBJETIVOS ESPECÍFICOS

- Administrar los riesgos de seguridad de la información para mantenerlos en niveles aceptables.
- Aplicar de manera correcta la legislación relacionada con la protección de datos personales
- Crear e implementar las políticas de seguridad y privacidad del Hospital Regional de Monquirá ESE.
- Implementar acciones correctivas y de mejora para el Sistema de Gestión de Seguridad de la Información y el Modelo de Seguridad y Privacidad de la Información, de Gobierno en Línea.
- Monitorear el cumplimiento de los requisitos de seguridad de la información, mediante el uso de herramientas de diagnóstico, revisiones por parte de la Alta Dirección y auditorías internas planificadas a intervalos regulares.
- Optimizar la gestión de la seguridad de la información al interior del Hospital Regional de Monquirá ESE.
- Optimizar la labor de acceso a la información pública
- Promover el uso de mejores prácticas de seguridad de la información en del Hospital Regional de Monquirá ESE.
- Promover el uso de mejores prácticas de seguridad de la información, para ser la base de aplicación del concepto de Seguridad Digital.
- Proteger los activos de información del Hospital Regional de Monquirá ESE, con base en los criterios de confidencialidad, integridad y disponibilidad.

	HOSPITAL REGIONAL DE MONIQUIRA E.S.E		
	FORMATO PLAN		
	PROCESO DE GESTIÓN DE TECNOLOGÍA		
	SUBPROCESO: SISTEMAS		
CÓDIGO:	GT-PL-02	VERSIÓN	V1-2023

- Revisar los roles relacionados con la privacidad y seguridad de la información al interior del Hospital Regional de Moniquirá ESE. para optimizar su articulación.
- Sensibilizar y capacitar a los servidores públicos, proveedores y partes interesadas acerca del Sistema de Gestión de Seguridad de la Información y el Modelo de Seguridad y Privacidad de la Información, de Gobierno en Línea, fortaleciendo el nivel de conciencia de estos, en cuanto a la necesidad de salvaguardar los activos de información institucionales.

4. ALCANCE DEL DOCUMENTO

El plan de Riesgos de Seguridad y Privacidad aplica a todos los procesos del Hospital Regional de Moniquirá ESE, los cuales manejen, procesen o interactúen con información institucional. Este documento está dirigido a los colaboradores administrativos, asistenciales, contratistas, y demás miembros del Hospital Regional de Moniquirá ESE, incluyendo al personal vinculado con empresas que prestan servicios al hospital que utilizan tecnologías de información. Este plan incluye a los equipos propios, arrendados, tercerizados que se encuentren en el hospital y que sean conectados a las redes del hospital.

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.


5. DEFINICIONES

Activos de Información: Se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas...) que tenga valor para la organización.

Aviso de Privacidad: Comunicación verbal o escrita generada por el responsable, dirigida al Titular para el tratamiento de sus datos personales, mediante la cual se le informa acerca de la existencia de las políticas de tratamiento de información que le serán aplicables, la forma de acceder a las mismas y las finalidades del tratamiento que se pretende dar a los datos personales.

Identificación De Activos De Información: Es un código para ordenar y localizar los activos de información.

Este documento es propiedad del Hospital Regional de Moniquirá E.S.E. Copias consultadas fuera del SGC no tienen validez. El uso de la información es exclusivo al interior de la Institución para el desarrollo de las funciones encomendadas. Está prohibido divulgar y reproducir total o parcialmente este documento.

	HOSPITAL REGIONAL DE MONIQUIRA E.S.E		
	FORMATO PLAN		
	PROCESO DE GESTIÓN DE TECNOLOGÍA		
	SUBPROCESO: SISTEMAS		
CÓDIGO:	GT-PL-02	VERSIÓN	V1-2023

Clasificación De Información: Es la clasificación que se debe dar en función de los requisitos legales, valor, criticidad, y susceptibilidad a divulgación o modificaciones no autorizadas.

Integridad: La información y sus métodos de procesamiento deben ser completos y exactos.

Disponibilidad: La información y los servicios deben estar disponibles en el momento que sea requerido.

Confidencialidad: La información debe ser accesible sólo a aquellas personas autorizadas.

Control: 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.

Dato Personal: Es cualquier pieza de información vinculada a una o varias personas determinadas o determinables o que puedan asociarse con una persona natural o jurídica.

Los datos impersonales no se sujetan al régimen de protección de datos de la presente ley.


Dato Público: 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.

Dato Semiprivado: Es el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio de actividad comercial o de servicios.

Dato Privado: Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular.

Dato Sensible: 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

	HOSPITAL REGIONAL DE MONIQUIRA E.S.E		
	FORMATO PLAN		
	PROCESO DE GESTIÓN DE TECNOLOGÍA		
	SUBPROCESO: SISTEMAS		
CÓDIGO:	GT-PL-02	VERSIÓN	V1-2023

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.

Documento en Construcción: Es aquella información preliminar o no definitiva.

(artículo 6, literal k Ley 1712 de 2014).


Información Clasificada: Es aquella información que estando en poder o custodia de un sujeto, 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 de manera motivada y por escrito, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados estipulados en el artículo 18 de la Ley 1712 de 2014 y su acceso pudiere causar un daño a los siguientes derechos:

- a. El derecho de toda persona a la intimidad, bajo las limitaciones propias que impone la condición de servidor público, en concordancia con lo estipulado;
- b. El derecho de toda persona a la vida, la salud o la seguridad;
- c. Los secretos comerciales, industriales y profesionales, así como los estipulados en el parágrafo del artículo 77 de la Ley 1474 de 2011.

Estas excepciones tienen una duración ilimitada y no deberán aplicarse cuando la persona natural o jurídica ha consentido en la revelación de sus datos personales o privados o bien cuando es claro que la información fue entregada como parte de aquella información que debe estar bajo el régimen de publicidad aplicable. (Artículo 6, literal c y 18 Ley 1712 de 2014).

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 de manera motivada y por escrito, por daño a intereses públicos y bajo el cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. Se podrá negar el acceso a esta información cuando concurra una de las siguientes circunstancias y siempre que dicho acceso estuviere expresamente prohibido por una norma legal o constitucional:

- a. La defensa y seguridad nacional;
- b. La seguridad pública;
- c. Las relaciones internacionales;
- d. La prevención, investigación y persecución de los delitos y las faltas disciplinarias, mientras que no se haga efectiva la medida de aseguramiento o se formule pliego de cargos, según el caso;
- e. El debido proceso y la igualdad de las partes en los procesos judiciales;

	HOSPITAL REGIONAL DE MONIQUIRA E.S.E		
	FORMATO PLAN		
	PROCESO DE GESTIÓN DE TECNOLOGÍA		
	SUBPROCESO: SISTEMAS		
CÓDIGO:	GT-PL-02	VERSIÓN	V1-2023

- f. La administración efectiva de la justicia;
- g. Los derechos de la infancia y la adolescencia;
- h. La estabilidad macroeconómica y financiera del país;
- i. La salud pública.

Se exceptúan también los documentos que contengan las opiniones o puntos de vista que formen parte del proceso deliberativo de los servidores públicos.


(Artículo 6, literal d y artículo 19 Ley 1712 de 2014).

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.


6. MARCO NORMATIVO

Las Normas a considerar en lo referente al del Hospital Regional de Moniquirá ESE. Y el Ministerio de las TIC son las siguientes:

- Acuerdo 03 de 2015 del Archivo General de la Nación Lineamientos generales sobre la gestión de documentos electrónicos
- Acuerdo 03 de 2015 del Archivo General de la Nación Lineamientos generales sobre la gestión de documentos electrónicos Pagina 7 de 13
- Anexo 1 - Resolución 3564 de 2015 - Reglamenta aspectos relacionados con la Ley de Transparencia y Acceso a la Información Pública
- Decreto 008 de 2013 por el cual se reestructura el Nivel central de la Gobernación de Cundinamarca.
- Decreto 019 de 2012 - Suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública
- Decreto 019 de 2012 Supresión de trámites
- Decreto 1377 de 2013: Protección de datos
- Decreto 1747 de 2000 - Entidades de certificación, los certificados y las firmas digitales
- Decreto 2364 de 2012 - Firma electrónica
- Decreto 2609 de 2012 Decreto con el cual se suministran las directrices para los sistemas de gestión documental en las instituciones nacionales.
- Decreto 2693 de 2012 Estrategia Gobierno en Línea.

	HOSPITAL REGIONAL DE MONIQUIRA E.S.E		
	FORMATO PLAN		
	PROCESO DE GESTIÓN DE TECNOLOGÍA SUBPROCESO: SISTEMAS		
	CÓDIGO:	GT-PL-02	VERSIÓN

- Decreto 619 del 28 de diciembre de 2007, Se establece la estrategia de Gobierno Electrónico de los organismos y de las entidades del Departamento.
- Decreto Ley 2150 de 1995 - Suprimen y reforman regulaciones, procedimientos o trámites innecesarios existentes en la Administración Pública
- Decreto Nacional 1151 del 14 de abril de 2008- Manual para la implementación de la estrategia de gobierno en línea de la República de Colombia. Por medio del cual se establecen los lineamientos generales de la estrategia de Gobierno en Línea de la República de Colombia, se reglamenta parcialmente la Ley 962 de 2005, y se dictan otras disposiciones.
- Decreto número 1078 de 2015
- Decreto número 2573 de 2014
- Decreto número 415 de 2016
- Decreto Reglamentario Único 1081 de 2015 - Reglamento sobre la gestión de la información pública
- Directiva 022 de 2011. Estandarización de la información de identificación, caracterización, ubicación y contacto de los ciudadanos y ciudadanas que capturan las entidades del Departamento.
- Directiva 305 de 20 de octubre de 2008. Por la cual se expiden políticas públicas en materia de TIC, respecto a planeación, seguridad, democratización, calidad, racionalización del gasto, conectividad, infraestructura de datos espaciales y software libre.
- Ley 1266 de 2008 - Disposiciones generales de habeas data y se regula el manejo de la información
- Ley 1341 de 2009, Masificación de Gobierno en Línea.
- Ley 1437 de 2011: Código de Procedimiento Administrativo y de lo Contencioso Administrativo
- Ley 1450 de 2011, Artículo 227. Bases de datos y seguridad de la Información en PND
- Ley 1712 de 2014 - Ley de Transparencia y acceso a la información pública
- Ley 1712 de 2014 - Ley de Transparencia y acceso a la información pública
- Ley 527 de 1999 - Ley de Comercio Electrónico
- Ley 57 de 1985 -Publicidad de los actos y documentos oficiales
- Ley 594 de 2000 - Ley General de Archivos
- Ley 962 de 2005 - Racionalización de trámites y procedimientos administrativos procedimientos administrativos
- Ley anti-trámites (Decreto-ley 19 de 2012)
- Ley Estatutaria 156. Por medio de la cual, se crea la Ley de transparencia y del derecho de acceso a la información pública nacional. Con el objeto de regular el derecho de acceso a información pública entre otros.
- Ley Estatutaria 1581 de 2012 - Protección de datos personales
- Ley estatutaria 1618 de 2013: Ejercicio pleno de las personas con discapacidad

	HOSPITAL REGIONAL DE MONIQUIRA E.S.E		
	FORMATO PLAN		
	PROCESO DE GESTIÓN DE TECNOLOGÍA		
	SUBPROCESO: SISTEMAS		
CÓDIGO:	GT-PL-02	VERSIÓN	V1-2023

- Ley Estatutaria 1757 de 2015 - Promoción y protección del derecho a la participación democrática
- Ley Estatutaria 1757 de 2015 - Promoción y protección del derecho a la participación democrática
- NTC ISO/IEC 17799 (ISO 27002)
- NTC-ISO/IEC 27001
- Ordenanza 128 del 2012 "Por el cual se adopta el Plan de Desarrollo Departamental.
- Título 9 - Decreto 1078 de 2015 - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones

7. DESCRIPCIÓN DEL PLAN

El grupo de colaboradores del Hospital Regional de Moniquirá ESE, y la gerencia del Hospital, se comprometen a garantizar la confidencialidad, seguridad e integridad de la información de los usuarios y su familia, clientes internos y externos en cuanto a seguridad lógica y física de los activos de la información, fomentando canales de comunicación que garanticen acceso y transparencia de la información pública a través de uso adecuado de las TICS, cumpliendo con las disposiciones generales para la protección de datos, aportando al cumplimiento de la Misión, Visión y objetivos estratégicos del hospital.


8. ACCIONES DE MEJORAMIENTO

- Definir cronograma de actividades para identificar el estado actual de la organización con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información
- Encuesta de seguridad
- Estratificación
- Autodiagnóstico de cumplimiento de la ley de protección de datos personales
- Autoevaluación del Modelo de Seguridad de la Información
- Aplicar las guías según cronograma establecido
- Socializar los hallazgos encontrados a la alta dirección.
- Realizar acciones según resultados de efectividad obtenidos

9. BARRERA DE MEJORAMIENTO Y CONTROL PROPUESTO

Bajo conocimiento en la implementación de este tipo de planes

Este documento es propiedad del Hospital Regional de Moniquirá E.S.E. Copias consultadas fuera del SGC no tienen validez. El uso de la información es exclusivo al interior de la Institución para el desarrollo de las funciones encomendadas. Está prohibido divulgar y reproducir total o parcialmente este documento.

	HOSPITAL REGIONAL DE MONIQUIRA E.S.E		
	FORMATO PLAN		
	PROCESO DE GESTIÓN DE TECNOLOGÍA		
	SUBPROCESO: SISTEMAS		
CÓDIGO:	GT-PL-02	VERSIÓN	V1-2023

Subjetividad en el levantamiento de la información

10. FASE DIAGNOSTICO

Compromiso de Apoyo al SGSI y al MSPI.

Partes Interesadas Pertinentes al MSPI/SGSI del Hospital Regional de Moniquirá ESE.

11. FASE PLANIFICACIÓN


Política y Objetivos del SGSI y el MSPI

Manual de Políticas de Seguridad de la Información

Informe Inventario de Activos de Información del Hospital Regional de Moniquirá ESE.


12. PLAN DE ACCIÓN

ID	Actividad	Responsable	Indicador	Fecha de cumplimiento
1	Definir cronograma de actividades para identificar el estado actual de la organización con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información	Eduardo Mateus Camacho	Cronograma aprobado	30/04/2023
2	Encuesta de seguridad	Eduardo Mateus Camacho	Encuesta realizada	30/04/2023
3	Estratificación	Eduardo Mateus Camacho	Estratificación Realizada	30/06/2023

	HOSPITAL REGIONAL DE MONIQUIRA E.S.E		
	FORMATO PLAN		
	PROCESO DE GESTIÓN DE TECNOLOGÍA		
	SUBPROCESO: SISTEMAS		
CÓDIGO:	GT-PL-02	VERSIÓN	V1-2023


4	Autodiagnóstico de cumplimiento de la ley de protección de datos personales	Eduardo Mateus Camacho	Autodiagnóstico de cumplimiento realizado	30/06/2023
5	Autoevaluación del Modelo de Seguridad de la Información	Eduardo Mateus Camacho	Autoevaluación realizada	30/09/2023
6	Aplicar las guías según cronograma establecido	Eduardo Mateus Camacho	Guías establecidas / Guías aplicadas	30/09/2023
7	Socializar los hallazgos encontrados a la alta dirección.	Eduardo Mateus Camacho	Registro de Socialización.	31/12/2023
8	Realizar acciones según resultados de efectividad obtenidos	Eduardo Mateus Camacho	Acciones de efectividad realizadas.	31/12/2023

El presente plan se aprobó en Comité Institucional de Gestión y Desempeño realizado el 31 de enero de 2023 y mediante Resolución 010 de 2023

	HOSPITAL REGIONAL DE MONIQUIRA E.S.E			
	FORMATO PLAN			
	PROCESO DE GESTIÓN DE TECNOLOGÍA			
	SUBPROCESO: SISTEMAS			
	CÓDIGO:	GT-PL-02	VERSIÓN	V1-2023

12. CRONOGRAMA

Cronograma de Actividades Plan de Seguridad y Privacidad de la Información												
Actividad	mar-2023	abr-2023	may-2023	jun-2023	jul-2023	ago-2023	sep-2023	oct-2023	nov-2023	dic-2023	ene-2024	feb-2024
Realizar el Diagnóstico según MSPÍ												
Gestión de Activos												
Política de tratamiento de Datos												
Custodia de la Información												
Seguridad Física y Ambiental												
Relaciones con los Proveedores												
Aspectos de Seguridad de la Información en la gestión de continuidad												

	HOSPITAL REGIONAL DE MONIQUIRA E.S.E		
	FORMATO PLAN		
	PROCESO DE GESTIÓN DE TECNOLOGÍA		
	SUBPROCESO: SISTEMAS		
CÓDIGO:	GT-PL-02	VERSIÓN	V1-2023

CONTROL DE CAMBIOS.

Espacio de diligenciamiento en caso de requerir alguna actualización o cambio del documento

CONTROL DE CAMBIOS			
Versión	Descripción del Cambio	Aprobó	Fecha