	HOSPITAL REGIONAL DE MONIQUIRA E.S.E		
	FORMATO PLAN		
	PROCESO DE GESTIÓN DE LA TECNOLOGÍA		
	SUBPROCESO: SISTEMAS		
CÓDIGO:	GT-PL-03	VERSIÓN	V1-2023


PLAN DE TRATAMIENTO DE RIESGOS 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 LA TECNOLOGÍA SUBPROCESO: SISTEMAS		
	CÓDIGO:	GT-PL-03	VERSIÓN

CONTENIDO

1. Introducción	3
2. Objetivo del Plan.....	4
3. Objetivos Específicos.....	4
4. Alcance del Documento	4
5. Siglas y Definiciones.....	5
6. Marco Normativo	10
7. Análisis de la Situación Actual	12
7.1. Estrategia de TI.....	12
7.2. Uso y Apropiación de la Tecnología.....	13
8. Mapa de Riesgos de Corrupción	¡Error! Marcador no definido.
8.1. Gestión del Riesgo de Corrupción - Mapa de Riesgos de Corrupción	¡Error! Marcador no definido.
8.2. Identificación de Riesgos	¡Error! Marcador no definido.
8.3. Análisis de Riesgos	¡Error! Marcador no definido.
8.4. Valoración del Riesgo	¡Error! Marcador no definido.
8.5. Política de Administración de Riesgos	¡Error! Marcador no definido.
8.6. Seguimiento a Riesgos	¡Error! Marcador no definido.
8.7. Mapa de Riesgos	¡Error! Marcador no definido.
8.8. Indicadores y Riesgos	¡Error! Marcador no definido.
9. Actividades	18
10. Cumplimiento de Implementación	18
11. Cronograma.....	20
12. Seguimiento y Evaluación	¡Error! Marcador no definido.
13. Entregables	¡Error! Marcador no definido.
CONTROL DE CAMBIOS.	21

	HOSPITAL REGIONAL DE MONIQUIRA E.S.E		
	FORMATO PLAN		
	PROCESO DE GESTIÓN DE LA TECNOLOGÍA SUBPROCESO: SISTEMAS		
	CÓDIGO:	GT-PL-03	VERSIÓN

1. INTRODUCCIÓN


El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, tiene como finalidad ser un instrumento de mejora continua, implementa un método lógico y sistemático que permita identificar, analizar, evaluar, tratar, monitorear y comunicar los riesgos asociados el manejo de la información institucional, para lograr que estos no afecten de una manera relevante a la misma.

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

La metodología planteada, permitirá analizar lo que se tiene (Diagnostico), identificando las necesidades de la organización en cuanto al Tratamiento de Riesgos de Seguridad y Privacidad de la Información.

De igual manera este documento se debe actualizar de forma periódica (anual) y garantizando que se encuentre acorde a los objetivos estratégicos organizacionales <https://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html> .

	HOSPITAL REGIONAL DE MONIQUIRA E.S.E		
	FORMATO PLAN		
	PROCESO DE GESTIÓN DE LA TECNOLOGÍA SUBPROCESO: SISTEMAS		
	CÓDIGO:	GT-PL-03	VERSIÓN

2. OBJETIVO GENERAL DEL PLAN

Controlar y minimizar los riesgos asociados a la seguridad y privacidad de la información, con el fin de salvaguardar los activos de información, el manejo de medios, control de acceso y gestión de usuarios y así proteger la Confidencialidad, Integridad y Disponibilidad de la información, así como su privacidad tomando en cuenta tanto los procesos como de las personas vinculadas con la información de la institución


3. OBJETIVOS ESPECÍFICOS

- Lograr un diagnóstico real de la situación actual de la institución en materia de riesgos de seguridad y privacidad de la Información
- Aplicar las metodologías, mejores prácticas y recomendaciones dadas por la función pública DAPF, por el Ministerio de las TIC e ISO para el Tratamiento de Riesgos de Seguridad y Privacidad de la Información
- Diligenciar el instrumento MSPI de Ministerio de las TIC y documentar un plan de trabajo específico, conforme a los resultados de este instrumento.
- Dar cumplimiento a lo establecido por la ley 1581 de 2012 y demás normatividad vigente en cuanto a tratamiento de riesgos de seguridad y privacidad de la información.
- Identificar la ubicación y propietarios de los activos de información a través del inventario del mismo en donde se categorice y valore los activos de información.
- Establecer los controles y políticas de la seguridad de la información que garantice la Confidencialidad Integridad y Disponibilidad de la información.
- Crear el mapa de riesgos informáticos de la Hospital Regional de Moniquirá.

4. ALCANCE DEL DOCUMENTO

Para la realización del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, la Hospital Regional de Moniquirá, se utilizará la Guía 7 Gestión de riesgos y la Guía 8 Controles de seguridad de la información, el Modelo de Seguridad y Privacidad de la Información MinTIC, el Instructivo y el Instrumento de Evaluación MSPI y demás instrumentos proporcionados por las entidades relacionadas.

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 LA TECNOLOGÍA SUBPROCESO: SISTEMAS		
	CÓDIGO:	GT-PL-03	VERSIÓN

5. SIGLAS Y DEFINICIONES

CIO: Chief Information Officer

AE: Arquitectura Empresarial

Marco de Referencia de AE: Marco de Referencia de Arquitectura Empresarial para la Gestión de TI del Estado

TI: Tecnologías de la Información

Ámbito:

Área o temática que aborda un dominio y que agrupa temas comunes dentro del dominio. Es la segunda capa del diseño conceptual del Marco de Referencia de Arquitectura Empresarial.

Ambiente (de desarrollo, pruebas o producción):

Es la infraestructura tecnológica (hardware y software) que permite desarrollar, probar o ejecutar todos los elementos o componentes para ofrecer un servicio de Tecnologías de la Información.

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/IEC 27000).

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.


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).

Amenazas:

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

Capacidades de TI:

	HOSPITAL REGIONAL DE MONIQUIRA E.S.E		
	FORMATO PLAN		
	PROCESO DE GESTIÓN DE LA TECNOLOGÍA SUBPROCESO: SISTEMAS		
	CÓDIGO:	GT-PL-03	VERSIÓN

Son un subconjunto de las capacidades institucionales operativas que tienen como propósito asegurar el adecuado aprovisionamiento del talento humano y los recursos que se necesitan para ofrecer los servicios de TI definidos en su catálogo.

Dato:

Es una representación simbólica de una característica particular de un elemento o situación, que pertenece a un modelo de una realidad. Tiene un tipo (por ejemplo numérico, cadena de caracteres o lógico) que determina el conjunto de valores que el dato puede tomar. En el contexto informático, los datos se almacenan, procesan y comunican usando medios electrónicos. Constituyen los elementos primarios de los sistemas de información.

Esquema de Gobierno TI:

Es un modelo para la administración de las capacidades y servicios de TI de una institución. Incluye una estructura organizacional, un conjunto de procesos, un conjunto de indicadores y un modelo de toma de decisiones; todo lo anterior enmarcado en el modelo de gobierno de la entidad.

Estrategia TI:

Es el conjunto de principios, objetivos y acciones concretas que reflejan la forma en la cual una entidad decide utilizar las Tecnologías de la Información para permitir el logro de su misión de una manera eficaz. La Estrategia TI es una parte integral de la estrategia de una entidad.

Elemento:

Tema de relevancia que se destaca dentro de cada ámbito.

Flujo de información:

Corresponde a la descripción explícita de la interacción entre proveedores y consumidores de información, con un patrón repetible de invocación definido por parte de la entidad. Puede incorporar servicios de información, datos e información.


Función:

Responsabilidad o actividad inherente a un rol.

Guía:

Es una definición procedimental que determina, por medio de actividades, los pasos que se deben ejecutar para producir un resultado con unas ciertas características o propiedades. En el contexto informático, se utilizan para expresar metodologías de trabajo que reflejan las mejores prácticas.

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 LA TECNOLOGÍA		
	SUBPROCESO: SISTEMAS		
CÓDIGO:	GT-PL-03	VERSIÓN	V1-2023

Información:

Es un conjunto de datos organizados y procesados que tienen un significado, relevancia, propósito y contexto. La información sirve como evidencia de las actuaciones de las entidades. Un documento se considera información y debe ser gestionado como tal.

Indicador:

En el contexto de la informática, un indicador es una medida de logro de algún objetivo planteado.

Instrumento:

Es un medio o recurso que se puede utilizar en el desarrollo de acciones para lograr un resultado deseado.

Mesa de servicio o de ayuda:

Es una unidad funcional dedicada a gestionar una variedad de eventos sobre el servicio. La mesa puede ser un punto único de contacto para los usuarios de TI. Maneja los incidentes y solicitudes de servicio a través del uso de herramientas especializadas para dejar registro y administrar los eventos.

Mejores prácticas:

Conjunto de acciones que han sido implementadas con éxito en varias organizaciones, siguiendo principios y procedimientos adecuados.

Normatividad:


Leyes, decretos y demás desarrollos normativos que guían las acciones para implementar el Marco de Referencia de Arquitectura Empresarial para la gestión de TI.

Nube: Término usado para referirse a la computación en la nube (cloud computing). Trata de los servicios en la web que proveen características básicas y avanzadas de procesamiento y almacenamiento.

Objetivo: En un modelo estratégico, la visión se detalla como un conjunto de objetivos, cada uno de los cuales representa un propósito específico, medible, alcanzable, realista y con un tiempo definido. Un objetivo, a su vez, se especifica a través de un conjunto de metas.

Principios: Son un conjunto de enunciados expresados en forma de reglas de alto nivel, que guían una institución, permitiéndole tomar decisiones sobre una base sólida. Reflejan los valores y convicciones de una entidad, y deben ser interpretados

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 LA TECNOLOGÍA SUBPROCESO: SISTEMAS		
	CÓDIGO:	GT-PL-03	VERSIÓN

y usados como un conjunto. Los principios de TI definen la esencia estratégica de un PETI.

Proyecto: Es un conjunto estructurado de actividades relacionadas para cumplir con un objetivo definido, con unos recursos asignados, con un plazo definido y un presupuesto acordado.

Roles: Conjunto de responsabilidades y actividades asignadas a una persona o grupo de personas para apoyar la adopción y aplicación del Marco de Referencia de Arquitectura Empresarial para la gestión de TI.

Servicio de información: Consiste en la entrega de información de valor para los usuarios de una entidad a través de un proveedor de servicio interno o externo. Un servicio de información se describe a través de un contrato funcional (qué recibe como entrada y qué produce como salida) y un conjunto de acuerdos de servicio que debe cumplir.

Servicio Tecnológico: Es un caso particular de un servicio de TI que consiste en una facilidad directamente derivada de los recursos de la plataforma tecnológica (hardware y software) de la institución. En este tipo de servicios los Acuerdos de Nivel de Servicio son críticos para garantizar algunos atributos de calidad como disponibilidad, seguridad, confiabilidad, etc.


Servicio de TI: Es una facilidad elaborada o construida usando tecnologías de la información para permitir una eficiente implementación de las capacidades institucionales. A través de la prestación de estos servicios es que TI produce valor a la organización. Los servicios de información son casos particulares de servicios de TI. Los servicios de TI deben tener asociados unos acuerdos de nivel de servicio. Servicio institucional: Es un servicio ofrecido a los usuarios de la institución en cumplimiento de su misión y objetivos.

Datos Personales:

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

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 Manual de GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente.

	HOSPITAL REGIONAL DE MONIQUIRA E.S.E		
	FORMATO PLAN		
	PROCESO DE GESTIÓN DE LA TECNOLOGÍA SUBPROCESO: SISTEMAS		
	CÓDIGO:	GT-PL-03	VERSIÓN

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).

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).

Riesgo de seguridad de la información:

Posibilidad de que una amenaza concreta que pueda aprovechar una vulnerabilidad para causar una pérdida o daño en un activo de información; estos daños consisten en la afectación de la confidencialidad, integridad o disponibilidad de la información. Cuando la amenaza se convierta en una oportunidad se debe tener en cuenta en el beneficio que se genera. También se puede generar riesgo positivo en la seguridad de la información por el aprovechamiento de oportunidades y fortalezas que se presenten.

Riesgo Positivo:


Posibilidad de ocurrencia de un evento o situación que permita optimizar los procesos y/o la gestión institucional, a causa de oportunidades y/o fortalezas que se presentan en beneficio de la entidad.

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

	HOSPITAL REGIONAL DE MONIQUIRA E.S.E		
	FORMATO PLAN		
	PROCESO DE GESTIÓN DE LA TECNOLOGÍA		
	SUBPROCESO: SISTEMAS		
CÓDIGO:	GT-PL-03	VERSIÓN	V1-2023

de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).

Partes interesadas (Stakeholders):

Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad. (Ministerio de Tecnologías de la Información y las Comunicaciones, 2016, pág. 11)

Equipo de Cómputo:

El equipo de cómputo se refiere a los mecanismos y al material de computación que está adjunto a él. Puede incluir a los computadores personales (PC's), servidores de mediana escala, ordenadores centrales, dispositivos de almacenamiento, equipos de comunicaciones/internet, equipo de impresión, energía eléctrica y equipo para identificación personal.

Hardware:

Se refiere a la parte física del equipo, la parte tangible, la que se puede ver y tocar.

Software:


Estos son los programas informáticos que hacen posible la realización de tareas específicas dentro de un computador. Por ejemplo Word, Excel, los sistemas operativos, los navegadores de internet, etc.

6. MARCO NORMATIVO


Las Normas a considerar en lo referente al 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

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 LA TECNOLOGÍA SUBPROCESO: SISTEMAS		
	CÓDIGO:	GT-PL-03	VERSIÓN

- 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.
- 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 527 de 1999 - Ley de Comercio Electrónico
- Ley 594 de 2000 - Ley General de Archivos
- Ley 962 de 2005 - Racionalización de trámites y procedimientos administrativos
- Ley anti trámites (Decreto-ley 19 de 2012)

	HOSPITAL REGIONAL DE MONIQUIRA E.S.E		
	FORMATO PLAN		
	PROCESO DE GESTIÓN DE LA TECNOLOGÍA SUBPROCESO: SISTEMAS		
	CÓDIGO:	GT-PL-03	VERSIÓN

- 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
- 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. ANÁLISIS DE LA SITUACIÓN ACTUAL


En este apartado vemos la situación actual de las Tecnologías de la Información de la institución en relación con los dominios del marco de referencia de Arquitectura Empresarial. Este análisis nos permitirá conocer el estado actual o línea base a partir de la cual se debe partir para proyectar la visión de lo que se espera en materia de gestión de TI en el Hospital Regional de Moniquirá ESE.

El análisis se realiza teniendo en cuenta los siguientes componentes: Mapa de procesos y servicios, inventario de sistemas de información, inventario de la infraestructura, inventario de la plataforma, inventario de redes, lineamientos de gobierno en línea, valoración de la gobernabilidad y la seguridad de la información.

7.1. Estrategia de TI.

Actualmente la Hospital Regional de Moniquirá está en proceso de elaboración de una serie de Políticas de tecnologías de información que buscan gestionar la continuidad del negocio por medio de la implementación de procedimientos que aseguren la operación de los servicios e infraestructura, y también que éstos sean gestionados bajo estándares de seguridad y control de la información.

Esta implementación se adoptará gradualmente respecto a la consolidación del documento, no obstante, la entidad ha generado iniciativas que, aunque no estén contempladas en un dominio de Estrategia de Tecnologías de Información, si hacen

	HOSPITAL REGIONAL DE MONIQUIRA E.S.E		
	FORMATO PLAN		
	PROCESO DE GESTIÓN DE LA TECNOLOGÍA		
	SUBPROCESO: SISTEMAS		
CÓDIGO:	GT-PL-03	VERSIÓN	V1-2023

parte importante en el desarrollo de la misma, como lo es Gobierno Digital, Implementación de la norma ISO 27001:2013.

7.2. Uso y Apropiación de la Tecnología.

Para lograr un adecuado uso y apropiación de la tecnología, actualmente el Hospital Regional de Moniquirá ESE, realiza programas de inducción, capacitación y reinducción de acuerdo a con su plan de capacitaciones, pero todavía no lo hace sobre los procesos sistemas de información y herramientas tecnológicas, este será un ajuste que se le realizara próximamente; también cuenta en la página web, en la que se publican diversos contenidos institucionales para el aprendizaje, comprensión y apropiación procesos del hospital, pendiente los servicios TI; de igual forma se cuenta con una red local (Somos Remo) , la cual sirve como herramienta para que cada uno de los usuarios puedan tener acceso a información que tiene expuestos diversos temas sobre los servicios ofrecidos, próximamente se publicaran las políticas de seguridad de la información, uso de sistemas de información, entre otros documentos con contenido relevante para la institución.


Actualmente el hospital cuenta con una plataforma E-learning, plataforma elaborada en Moodle que le permitirá a todo el personal realizar cursos virtuales, que afiancen el conocimiento y posibiliten aplicar los temas relacionados con los servicios Tecnologías de Información.

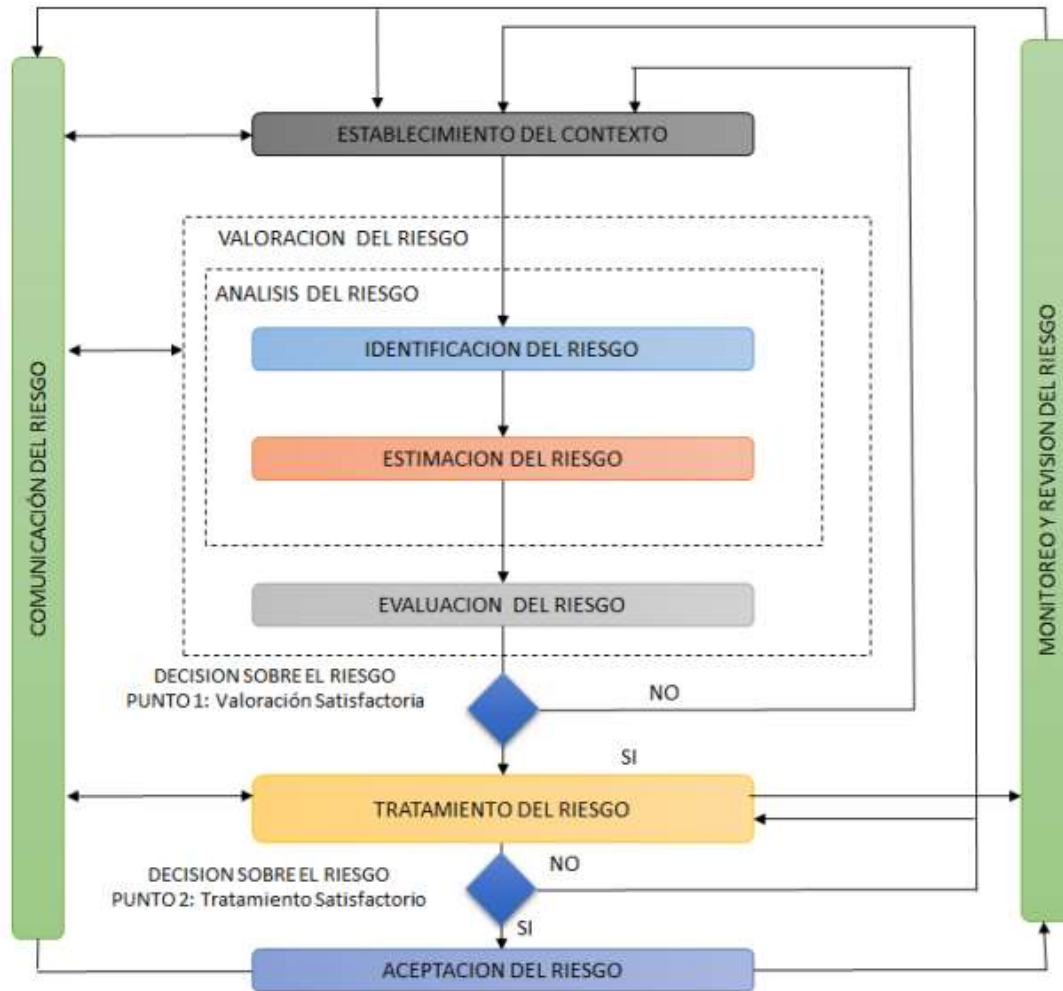
Con esta estrategia se busca que desde cada puesto de trabajo se tenga acceso a estos recursos académicos, importantes como elementos de educación y de sensibilización de cada uno de los usuarios en el manejo y transferencia de conocimiento para el desempeño de sus labores.

8. TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

Para identificar, valorar y establecer controles asociados a los riesgos de seguridad y privacidad de la información, la metodología de la gestión del riesgo del DAFP, en lo que respecta a esta tipología de riesgos, así como la identificación de activos de información según lo dispuesto por el Min Tic.

Figura 1. Metodología para la Gestión del riesgo de seguridad de la información según DAFP


	HOSPITAL REGIONAL DE MONIQUIRA E.S.E		
	FORMATO PLAN		
	PROCESO DE GESTIÓN DE LA TECNOLOGÍA		
	SUBPROCESO: SISTEMAS		
CÓDIGO:	GT-PL-03	VERSIÓN	V1-2023



Fuente: ISO 27005. Fuente: ISO 27005, citado en [http://www.uptc.edu.co/export/sites/default/gel/documentos/plan trata rie seg inf2020.pdf](http://www.uptc.edu.co/export/sites/default/gel/documentos/plan_trata_rie_seg_inf2020.pdf)

Para la estimación de los riesgos se tomará la siguiente escala de probabilidad:

Figura 2. Escala de probabilidad para medir riesgos


	HOSPITAL REGIONAL DE MONIQUIRA E.S.E		
	FORMATO PLAN		
	PROCESO DE GESTIÓN DE LA TECNOLOGÍA SUBPROCESO: SISTEMAS		
	CÓDIGO:	GT-PL-03	VERSIÓN

ESCALA DE PROBABILIDAD	
NIVEL	DESCRIPCION
1	Raro Evento que puede ocurrir sólo en circunstancias excepcionales, entre 0 y 1 vez en 1 semestre.
2	Improbable Evento que puede ocurrir en pocas de las circunstancias, entre 2 y 5 veces en un semestre.
3	Posible Evento que puede ocurrir en algunas de las circunstancias entre seis y 10 veces en 1 semestre.
4	Probable Evento que puede ocurrir en casi siempre entre 11 y 15 veces en 1 semestre.
5	Casi Seguro Evento que puede ocurrir en la mayoría de las circunstancias más de 15 veces en 1 semestre.

Fuente: Tomado de ISO 31000 citado en [http://www.uptc.edu.co/export/sites/default/gel/documentos/plan trata rie seg inf 2020.pdf](http://www.uptc.edu.co/export/sites/default/gel/documentos/plan_trata_rie_seg_inf_2020.pdf)

Para la valoración de impacto se tomará en cuenta los siguientes criterios:

Figura 3. Valoración de impacto de riesgos

	HOSPITAL REGIONAL DE MONIQUIRÁ E.S.E			
	FORMATO PLAN			
	PROCESO DE GESTIÓN DE LA TECNOLOGÍA			
	SUBPROCESO: SISTEMAS			
	CÓDIGO:	GT-PL-03	VERSIÓN	V1-2023


VALOR DE IMPACTO		
NIVEL	DESCRIPCIÓN	ESCALA
1 Insignificante	Impacta negativamente de forma leve la imagen y operación de un rol. No tiene impacto Financiero para la Universidad o sus procesos. Impacta negativamente, posibilidad de recibir multas.	>=1 y <=4
2 Menor	Impacta negativamente la imagen y de manera importante la operación de un proceso. Se pueden presentar sobrecostos debido a reprocesos a nivel de un proceso. Impacta negativamente, posibilidad de recibir multas.	>=5 y <=8
3 Moderado	Afecta negativamente la imagen Institucional a nivel regional por retrasos en la prestación de los servicios y la operación no sólo del proceso evaluado sino de otros procesos. Se pueden presentar sobrecostos por reprocesos y aumento de carga operativa, no sólo en el proceso evaluado sino a otros procesos. Impacta negativamente, posibilidad de recibir una investigación disciplinaria.	>=9 y <=12
4 Mayor	Imagen Institucional a nivel nacional afectada, al igual que la operación por el incumplimiento en la prestación de servicios de la Universidad o el cumplimiento de sus objetivos estratégicos. Se pueden presentar sobrecostos por reprocesos significativos para una sede seccional de la Institución. Impacta negativamente, posibilidad de recibir una investigación fiscal.	>=13 y <=16
5 Catastrófico	Imagen Institucional afectada a nivel nacional e Internacional. Impacta negativamente la operación y el cumplimiento en la prestación de los servicios de la Institución y el incumplimiento de sus objetivos estratégicos. Se pueden presentar sobrecostos debido a reprocesos y aumento de carga operativa importante en toda la Universidad. Impacta negativamente, posibilidad de recibir una intervención o sanción, por parte de entes de control o cualquier ente regulador.	>=17 y <= 20

Fuente: Tomado de ISO 31000 citado en

http://www.uptc.edu.co/export/sites/default/gel/documentos/plan_trata_rie_seg_inf2020.pdf

Para analizar los riesgos es necesario conciliar los impactos con las probabilidades, lo cual se hace en la matriz en la matriz IP:

Figura 4. Matriz Impacto-probabilidad.

	HOSPITAL REGIONAL DE MONIQUIRA E.S.E		
	FORMATO PLAN		
	PROCESO DE GESTIÓN DE LA TECNOLOGÍA SUBPROCESO: SISTEMAS		
	CÓDIGO:	GT-PL-03	VERSIÓN

MATRIZ IP

IMPACTO	VALOR	EVALUACION				
Catastrófico	5	5	10	15	20	25
Mayor	4	4	8	12	16	20
Moderado	3	3	6	9	12	15
Menor	2	2	4	6	8	10
Insignificante	1	1	2	3	4	5
	Valor	1	2	3	4	5
	PROBABILIDAD	Raro	Improbable	Posible	Probable	Casi Seguro

Matriz Impacto-probabilidad. Fuente: ISO 31000, citado en [http://www.uptc.edu.co/export/sites/default/gel/documentos/plan trata rie seg inf 2020.pdf](http://www.uptc.edu.co/export/sites/default/gel/documentos/plan_trata_rie_seg_inf_2020.pdf)


El diligenciamiento de la matriz IP permitirá a la entidad identificar los riesgos que deben ser priorizados para

Poder establecer los respectivos planes de acción y mitigación, los riesgos que se identifiquen en la zona roja, se consideran zona de alto riesgo y debe mitigarse de manera inmediata, los riesgos en la zona amarilla son de riesgo moderado y deben mitigarse en el corto y mediano plazo y los riesgos en la zona verde son de bajo riesgo y debe establecer planes de mitigación para intentar eliminarlo o identificar si se trata de un riesgo residual asociado al proceso.

Es necesario mencionar que la gestión integral de riesgos asociados a la seguridad y privacidad de la información debe estar siempre en concordancia con lo establecido en la política de gestión de riesgos institucional.

Se deben establecer los riesgos asociados a los procesos de TI y el plan de Mitigación de los mismos.

- Mejorar Continuamente la eficiencia, eficacia y efectividad del Hospital Regional de Moniquira ESE.
- Garantizar la Satisfacción de los usuarios de la Hospital Regional de Moniquira
- Contar con el recurso humano competente, en el manejo de la infraestructura tecnologías que sea suficiente para el cumplimiento de los objetivos misionales.
- Cumplir las metas e indicadores nacionales tecnológicos propuestos por el área de calidad y por el estado.

	HOSPITAL REGIONAL DE MONIQUIRA E.S.E		
	FORMATO PLAN		
	PROCESO DE GESTIÓN DE LA TECNOLOGÍA		
	SUBPROCESO: SISTEMAS		
CÓDIGO:	GT-PL-03	VERSIÓN	V1-2023

- Garantizar el cumplimiento de las actividades según las leyes y políticas del estado.
- Incrementar la participación, opinión, uso de medios disponibles en la página web, hacia la población en general.
- Generar iniciativas para la Racionalización de Trámites
- Generar mecanismos efectivos para optimizar la Rendición de Cuentas
- Generar mecanismos para mejorar la Atención al Ciudadano
- Generar mecanismos para la Transparencia y Acceso a la Información
- Igualmente, se realizara u del plan conforme a sus lineamientos internos y políticas del sector salud.


9. ACTIVIDADES

- 9.1. Realizar Diagnóstico
- 9.2. Elaborar el Alcance del Plan del Tratamiento de Riesgo de Seguridad y Privacidad de la Información
- 9.3. Realizar la Identificación de los Riesgos con los líderes del Proceso y entrevista con los líderes del Proceso.
- 9.4. Valorar del riesgo y del riesgo residual
- 9.5. Realizar Mapas de calor donde se ubican los riesgos
- 9.6. Plantear al plan de tratamiento de riesgo aprobado por los lideres

10. CUMPLIMIENTO DE IMPLEMENTACIÓN


De acuerdo con las fases mencionadas anteriormente, se describe a continuación los dominios que se deben desarrollar y los plazos de implementación de acuerdo con lo establecido por el Hospital Regional de Moniquira ESE.

- 10.1. Implementación de la Política de Seguridad.
- 10.2. Aspectos organizativos de la seguridad de la información
- 10.3. Seguridad Ligada a los recursos humanos
- 10.4. Revisión del Control de acceso
- 10.5. Seguridad en la operativa
- 10.6. Seguridad en las telecomunicaciones
- 10.7. Gestión de Incidentes de Seguridad de la Información
- 10.8. Aspectos de seguridad de la información en la gestión de continuidad del negocio.

	HOSPITAL REGIONAL DE MONIQUIRA E.S.E		
	FORMATO PLAN		
	PROCESO DE GESTIÓN DE LA TECNOLOGÍA SUBPROCESO: SISTEMAS		
	CÓDIGO:	GT-PL-03	VERSIÓN

11. PLAN DE ACCIÓN

ID	Actividad	Responsable	Indicador	Fecha de cumplimiento
1	Realizar el Diagnostico	Eduardo Mateus	Diagnostico Aprobado	30/04/2023
2	Elaborar el Alcance del Plan del Tratamiento de Riesgo de Seguridad y Privacidad de la Información	Eduardo Mateus	Alcance del Plan del Tratamiento de Riesgo de Seguridad y Privacidad de la Información Aprobado	30/06/2023
3	Realizar la Identificación de los Riesgos de seguridad y privacidad de la información	Eduardo Mateus	Riesgos de seguridad y privacidad de la información documentados	30/06/2023
4	Realizar la Identificación de los Riesgos de seguridad y privacidad de la información	Eduardo Mateus	Riesgos de seguridad y privacidad de la información documentados	30/06/2023
5	Valorar del riesgo y el riesgo residual	Eduardo Mateus	Riesgo residual establecido	30/10/2023
6	Realizar Mapas de calor donde se ubican los riesgos	Eduardo Mateus	Mapas de calor realizados	31/12/2023
7	Plantear al plan de tratamiento de riesgo aprobado por los lideres	Eduardo Mateus	Plan de tratamiento de riesgos aprobados	31/12/2023
8	Seguimiento y Control	Eduardo Mateus	Seguimiento y Control documentados y aprobados	31/12/2023


	HOSPITAL REGIONAL DE MONIQUIRA E.S.E			
	FORMATO PLAN			
	PROCESO DE GESTIÓN DE LA TECNOLOGÍA			
	SUBPROCESO: SISTEMAS			
	CÓDIGO:	GT-PL-03	VERSIÓN	V1-2023

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

12. CRONOGRAMA

Cronograma de Actividades Plan de Tratamiento de Riesgos 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												
Elaborar el Alcance del Plan del Tratamiento de Riesgo de Seguridad y Privacidad de la Información												
Realizar la Identificación de los Riesgos de seguridad y privacidad												

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 LA TECNOLOGÍA		
	SUBPROCESO: SISTEMAS		
CÓDIGO:	GT-PL-03	VERSIÓN	V1-2023