Tabla de contenido

1. INTRODUCCIÓN

El Hospital Departamental María Inmaculada (HDMI) gestiona un gran volumen de datos clínicos, administrativos y financieros, los cuales son fundamentales para la continuidad operativa y la calidad de la atención en salud. La creciente digitalización de los procesos hospitalarios ha traído consigo la necesidad de implementar estrategias efectivas que protejan la información ante amenazas internas y externas.

La seguridad de la información en el entorno hospitalario no solo es un requisito legal, sino también un pilar esencial para garantizar la confianza de los pacientes y la eficiencia de los procesos internos. En un contexto donde los ataques cibernéticos son cada vez más sofisticados, la protección de los datos se convierte en una prioridad para evitar fraudes, accesos indebidos y filtraciones que puedan comprometer la estabilidad del hospital y la privacidad de los pacientes.

En Colombia, la protección de los datos personales y sensibles está regulada por la Ley 1581 de 2012, que establece principios y normas para el tratamiento de la información. Asimismo, el Decreto 1072 de 2015 y la ISO 27001 establecen lineamientos sobre la seguridad y privacidad de la información en entidades del sector salud. El incumplimiento de estas disposiciones puede conllevar sanciones legales y afectar la confianza de los pacientes en la institución.

La información de los pacientes contiene datos altamente sensibles, por lo que es esencial adoptar medidas que eviten accesos no autorizados, alteraciones o pérdidas. La confidencialidad de la información médica no solo cumple con la normativa vigente, sino que también protege los derechos fundamentales de cada paciente. Un manejo inadecuado de estos datos puede derivar en consecuencias legales y afectar la reputación del hospital.

Asimismo, la adecuada administración de las credenciales de acceso por parte del personal hospitalario es crucial para minimizar riesgos asociados al mal uso o la divulgación indebida de datos. Los trabajadores deben ser conscientes de la importancia de mantener las credenciales seguras y de seguir buenas prácticas en el acceso y uso de los sistemas informáticos del hospital. La implementación de autenticación multifactorial, permisos restringidos según el rol del usuario y controles de auditoría son medidas clave para prevenir accesos no autorizados.

Por otro lado, la información administrativa y financiera del hospital debe resguardarse de posibles ataques o fraudes que puedan comprometer su estabilidad operativa y el cumplimiento de los requisitos regulatorios. La corrupción o alteración de estos datos podría generar pérdidas económicas significativas, afectar la toma de decisiones y comprometer la asignación eficiente de recursos. La implementación de protocolos de seguridad robustos, auditorías constantes y la formación del personal en ciberseguridad fortalecerán la resiliencia de la institución frente a estos desafíos.

Este plan establece un marco de referencia para la gestión de los riesgos tecnológicos en el HDMI, alineado con el Plan Estratégico de Tecnologías de Información (PETI). Su implementación permitirá reducir vulnerabilidades, mejorar la capacidad de respuesta ante incidentes y fomentar una cultura de protección de la información en toda la organización. Además, busca fortalecer la estructura organizativa en torno a la seguridad de la información, promoviendo una gestión eficiente y segura de los datos, garantizando el cumplimiento de las regulaciones y asegurando la continuidad operativa del hospital.

2. OBJETIVO

2.1 General

Garantizar la seguridad y privacidad de la información del hospital mediante un enfoque integral de gestión de riesgos, alineado con el Plan Estratégico de Tecnologías de Información (PETI).

2.2 Objetivos Específicos

- Identificar y evaluar los riesgos asociados a la seguridad de la información en los sistemas del hospital.
- Implementar medidas de mitigación para reducir vulnerabilidades y amenazas.
- Asegurar la interoperabilidad segura entre los sistemas de información
- Cumplir con normativas nacionales e internacionales de seguridad de la información.
- Monitorear y actualizar constantemente las estrategias de seguridad y privacidad.

3. TÉRMINOS Y DEFINICIONES

- **Riesgo:** Posibilidad de que ocurra un incidente que afecte la seguridad de la información.
- **Amenaza:** Cualquier factor o evento que pueda explotar una vulnerabilidad.
- **Tipos de amenazas:**
  - **Amenazas internas:** Errores humanos, accesos no autorizados de empleados, negligencia en la gestión de credenciales.
  - **Amenazas externas:** Ciberataques, malware, phishing, accesos indebidos por terceros.
  - **Desastres naturales**: Inundaciones, incendios, fallos eléctricos que afecten la infraestructura tecnológica.

- **Vulnerabilidad:** Debilidad o falla que puede ser explotada por una amenaza.
- **Confidencialidad**: Garantía de que la información solo es accesible por personas autorizadas.
- **Integridad:** Protección contra modificaciones no autorizadas de la información.
- **Disponibilidad:** Asegurar que la información y los sistemas estén accesibles cuando se necesiten.
- **Autenticación:** Proceso de verificación de identidad para el acceso a sistemas de información.
- **Cifrado**: Técnica de protección de datos mediante algoritmos que impiden su lectura sin autorización.

- **Control perimetral:** Estrategias de seguridad física y lógica para evitar accesos no autorizados a la red del hospital.
- **Centro de datos:** Instalación donde se almacenan y gestionan los servidores y sistemas críticos de información del hospital.
- **Cableado de datos:** Infraestructura física que permite la conectividad y el tráfico seguro de información dentro del hospital.
- **WLAN (Wireless Local Area Network):** Red inalámbrica interna que permite la comunicación y acceso a los sistemas hospitalarios.
- **Usuarios:** Personal autorizado para acceder a los sistemas de información del hospital, con diferentes niveles de permisos según su rol.

4. MARCO NORMATIVO O BASE LEGAL

Este plan de tratamiento de riesgos de seguridad y privacidad de la información está basado en el marco normativo y legal vigente en Colombia, asegurando el cumplimiento de las regulaciones aplicables al sector salud y la salvaguarda de los datos personales. A continuación, se presentan las principales normativas que rigen esta materia:

- **Constitución Política de Colombia (1991):** Establece el derecho a la intimidad y la protección de datos personales en su artículo 15, garantizando el acceso y manejo responsable de la información de los ciudadanos.
- **Ley 1581 de 2012:** Regula la protección de datos personales en Colombia, estableciendo principios de confidencialidad, seguridad y acceso restringido a la información de los pacientes.
- **Ley 1438 de 2011:** Refuerza el sistema de seguridad social en salud y promueve el uso de las TIC para mejorar la prestación de servicios de salud.
- **Ley 2015 de 2020:** Obliga la interoperabilidad de la Historia Clínica Electrónica (HCE), garantizando que los datos de los pacientes sean accesibles de manera segura y eficiente en todo el sistema de salud.
- **Ley 1753 de 2015:** Plan Nacional de Desarrollo que establece lineamientos estratégicos para la transformación digital del sector público y la interoperabilidad de sistemas de información en salud.
- **Ley 1341 de 2009:** Regula el desarrollo y promoción de las TIC en Colombia, asegurando su uso eficiente en entidades públicas y privadas.
- **Decreto 1078 de 2015:** Regula la estrategia de Gobierno Digital en Colombia, estableciendo directrices para la digitalización de los procesos administrativos y de atención al ciudadano en las entidades públicas.**Decreto 1008 de 2018**: Define los lineamientos generales para la política de Gobierno Digital,
- impulsando la modernización de las entidades estatales mediante el uso de tecnologías digitales.
- **Decreto 415 de 2016:** Fortalece la ciberseguridad y la protección de datos en entidades del Estado, estableciendo medidas para garantizar la integridad de la información y prevenir riesgos digitales.
- **Normas ISO 27001 y 27799:** Estándares internacionales que establecen las mejores prácticas en gestión de seguridad de la información y protección de datos en el sector salud.
- **CONPES 3854 de 2016**: Política Nacional de Seguridad Digital, orientada a fortalecer la ciberseguridad en entidades públicas y privadas.
- **Modelo de Seguridad, Protección y Privacidad de la Información (MSPI):** Garantiza la integridad, disponibilidad y confidencialidad de la información en entidades públicas.
- **Decreto 1499 de 2017**: Obliga a todas las entidades estatales a implementar el MSPI como parte del Modelo Integrado de Planeación y Gestión (MIPG), asegurando la protección de datos y la ciberseguridad en la gestión institucional.

Este marco normativo y legal orienta la formulación de estrategias de seguridad en el Hospital Departamental María Inmaculada, asegurando la protección de la información de los pacientes, la correcta gestión de los datos administrativos y financieros, y el cumplimiento de las obligaciones legales en materia de privacidad y seguridad de la información.

5. Responsable

- Gerencia
- Funcionarios HDMI

- Área de sistemas

6. INDICADORES

6.1 RIESGOS EN EL PROCESO TECNOLOGÍA E INFORMACIÓN

No.	RIESGOS	CAUSAS	CONTROLES A LOS RIESGOS	SOPORTES O EVIDENCIAS	IMPACTO
1 RIESGO (63)	Acceso indebido a los sistemas de información	Uso inadecuado de credenciales, compartir usuarios y contraseñas, adicional ausencia de cambios periódicos en las claves de acceso	1. El ingeniero de sistemas responsable de la creación de usuarios verifica, cada solicitud de apertura enviada por el área de Talento Humano, la identidad del funcionario mediante su presentación personal ante la oficina de Tecnología e Información. Con base en esta validación, se asignan los roles y accesos de acuerdo con las funciones a desempeñar. Este proceso queda registrado en el listado generado a través del formato TI-F-01 y en el acta de socialización de las políticas de seguridad de la información institucional.	formato TI-F-01 y acta de la socialización de las políticas de seguridad de la información institucional diligenciada y firmada por el nuevo funcionario, aceptando que se le expone y reconoce los compromisos adquiridos.	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos
		Falta de control de usuarios por parte del área de sistemas	El área de sistemas, de forma trimestral, compara los listados proporcionados por la oficina de Talento Humano (ya sea por ticket o correo electrónico) con los diferentes servicios, con el fin de identificar usuarios inactivos o aquellos que están siendo utilizados por personas incorrectas. Los hallazgos obtenidos se registran en un informe de usuarios dentro del sistema, incluyendo también las novedades reportadas por el área de Talento Humano.	Listado emitido por correo/mesa de ayuda el área de talento Humano relacionando el personal inactivo o retirado de la institución.	

2 RIESGO(64)	Pérdida de información en procesos administrativos	No elaborar el plan de mantenimiento preventivo y correctivo, el cual tiene como objetivo prevenir daños en los equipos e identificar la vida útil de otros.	Los técnicos de sistemas revisan, en cada evento reportado (correctivo) o programado (preventivo), el funcionamiento del equipo y sus componentes. También verifican en el sistema de información digital los activos fijos y su vida útil. Esta información facilita la toma de decisiones para gestionar la baja de un equipo de cómputo debido a obsolescencia o daños. El registro de los hallazgos o el control se realiza mediante la plataforma GLPI (ticket)	Registros en la plataforma de Ticket o mesa de ayuda. Registro en el Indicador TI-10	Impacto en la gestión administrativa y operativa del hospital
		No tener alternativas de almacenamiento de información	2. Los Técnicos de sistemas realizan en cada requerimiento atendido a las áreas administrativas y asistenciales la socialización de las políticas de seguridad de la información recalcando la salvaguarda de la información en la nube One Drive y carpetas direccionadas desde el servidor. Evidencia del anterior control es el acta de socialización realizada- MC-F-03	acta de socialización realizada- MC-F-03	
		Posibilidad que se presente daños en el DataCenter, y falta de espacio para salvaguardar información	3. El Profesional y Jefe del área de Sistemas realiza la supervisión del mantenimiento al DataCenter y verificación capacidad de almacenamiento. Reportado a través de la plataforma de ticket o mesa de ayuda el informe digital o físico entregado por el profesional que realiza dicha labor. Este informe será presentados a la dirección de la institución con el ánimo de informar o solicitar recursos. (se presentará un informe o	Informe anual de supervisión.	

			acta de alguna revisión que se realice al DataCenter principal o alguno novedad que se genere en este tema)		
3 RIESGO(65)	Interrupción de cualquier servicio que afecte la infraestructura tecnológica de la entidad por causas internas o externas.	Inconvenientes de configuración y direccionamiento en elementos y dispositivos que conforman la infraestructura de la red de datos. Bloqueos de Hardware y Software.	1. El profesional encargado de la Administración de las redes de Datos y/o Telecomunicaciones y los técnicos de Sistemas mediante la ejecución de los cronogramas establecidos para los mantenimientos preventivos a los equipos de cómputo de acuerdo con lo que establece el procedimiento para dicho mantenimiento preventivo. Reportado a través de la plataforma de Ticket o mesa de ayuda. (implementar cronograma mant. preventivos a los centros datos y cableados, de igual manera a las impresoras y Scanner)	*Publicación de Cronogramas de mantenimiento preventivo, *Reporte de mantenimiento preventivo. *Indicador Porcentaje de los Mantenimientos Preventivos.	EL IMPACTO : afecta directamente la atención del servicio a los usuarios, por consiguiente la buena imagen de la entidad se ve afectada

		Interrupción del servicio por parte del Proveedor del Sistema de Información Digital para Historias clínicas e información administrativa, S.I para imágenes Diagnosticas, servicio de internet, Correo electrónico y Pagina Web. Posibles daños externos en la infraestructura en la red de Datos por Terremoto, inundación, incendio o animales roedores.	2. El profesional y Jefe del área de sistemas realiza la supervisión a los contratos firmados que tiene la institución con los diferentes proveedores para los sistemas información digital, servicios de canal dedicado para internet, correo electrónico y pagina web, a través de comunicados, mediante el correo electrónico institucional. (con este control, debemos notificar con anterioridad mediante memorando o correo electrónico de algún mantenimiento o intervención que los proveedores realicen a dicho sistema)	*Contratos firmados con los proveedores. *Ante la interrupción del servicio se tendrán Comunicados institucionales mediante el correo electrónico.	
		Uso Inadecuado y seguridad de los equipos de computo por parte de los funcionarios o personal externo (aquí también nos referimos a los daños o atentados de terceras personas hacia nuestra infraestructura tecnológica. ejemplo: robos o daños	3. Socializar la Guía para el manejo y uso adecuado de los equipos de computo TI-I-03 con le personal administrativo y asistencial. (esto ya se realiza)	*Acta de socialización Guía para el manejo y uso adecuado de los equipos de computo TI-I-03	EL IMPACTO : afecta directamente la atención del servicio a los usuarios

4 RIESGO(66)	Posibilidad de Bloqueo de los sistemas de información, equipos de cómputo por desactualización Tecnológica	Cambios en la necesidad del servicio y la normatividad que obligue a Implementar actualizaciones con nuevas tecnologías. Evolución y mejora continua de la tecnología en cuanto a Hardware y Software. Falta de contrato con proveedores de software, Falta de contrato de mantenimiento de hardware.	1. El profesional y jefe del área de sistemas, verifica la necesidad y posibilidad de una mejora o actualización en los S.I y software, que a la vez será remitido a la dirección de la institución para su aprobación. De igual manera realiza la supervisión a los contratos firmados que tiene la institución con los proveedores para el sistema de información digital, servicios de canal dedicado para internet, correo electrónico, página Web y contratos de compra de equipos de cómputo para renovación.	*Contratos de soporte sistemas de información, Contrato de servicio de correo electrónico y página web. *Informe de supervisión de acuerdo a lo estipulado dentro de cada contrato.	EL IMPACTO: afecta directamente la atención del servicio a los usuarios, por consiguiente la buena imagen de la entidad se ve afectada
			2. De igual manera el profesional realiza la trazabilidad del tiempo de uso y actualizaciones de los equipos de cómputo, mediante las hojas de vida de los equipos, medición del indicador TI-11 Obsolescencia de equipos, mediante el inventario de los equipos de cómputo. Estas mejoras o actualizaciones se van desarrollando de acuerdo con las exigencias en la necesidad de los servicios que ofrece la institución.	*Hojas de vida de computo *indicador TI-11 Obsolescencia de equipos.	

6.2 INDICADORES

COD.	NOMBRE	% con el cual se cumple y % mínimo	FRECUENCIA DE MEDICION

TI-03 CDG 115	Porcentaje de efectividad de solicitudes por medio de tickets	SE CUMPLE CON EL 80% - MÍNIMO 70 %	trimestral
TI-10 CDG 140	Porcentaje de mantenimientos realizados a los de equipos (Pc, Impresoras y Scanner)	se cumple con el 90% - mínimo 80 %	trimestral
TI-08 CDG 140	Porcentaje Avance en la implementación del SGSI (Sistema de Gestión de la Seguridad de la Información)	SE CUMPLE CON EL 40% - MÍNIMO 25%	Se mide semestral, pero también se debe enviar evidencias de cumplimiento al poa(plan operativo anual)cada 3 meses..
TI-11 CDG 140	Obsolescencia de equipos de cómputo (PC, impresoras, escanner)	SE CUMPLE CON EL 15% - MINIMO 5%	SE MIDE ANUAL

7. ESTRUCTURA DOCUMENTAL

7.1 ALCANCE

El presente Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información del Hospital Departamental María Inmaculada (HDMI) abarca todos los procesos, infraestructuras, tecnologías y personal involucrado en la gestión, almacenamiento, procesamiento y transmisión de información dentro de la institución.

Este plan aplica a:

- Todos los sistemas de información utilizados en el hospital, incluyendo los clínicos, administrativos y financieros.
- Todos los niveles de personal, desde directivos hasta personal operativo, que accedan, manejen o administren información institucional.
- Infraestructura tecnológica, incluyendo servidores, redes, dispositivos de almacenamiento y mecanismos de seguridad digital.
- Políticas y procedimientos de seguridad orientados a la prevención, mitigación y control de riesgos de seguridad y privacidad de la información.
- Proveedores y terceros que tengan acceso o manejen información del hospital bajo cualquier modalidad contractual.
- Cumplimiento de normativas nacionales e internacionales en materia de protección de datos y ciberseguridad.

El alcance del plan se extiende a todas las áreas del hospital donde se gestionen datos críticos y se implementen medidas para minimizar riesgos asociados a accesos no autorizados, ataques cibernéticos, filtraciones de información, fallos operativos y cualquier otra amenaza que comprometa la seguridad y privacidad de la información hospitalaria.

7.2. METODOLOGÍA:

7.2.1 POLÍTICA DE ADMINISTRACIÓN DE RIESGOS

El Hospital Departamental María Inmaculada (HDMI) se compromete a mantener una cultura de gestión del riesgo que permita fortalecer las medidas de prevención, monitoreo y seguimiento al control para mitigar la posible ocurrencia de riesgos en las actividades desarrolladas por la institución. Esto incluye la responsabilidad de diseñar, adoptar y promover las políticas, planes, programas, iniciativas y proyectos del sector TIC, mediante mecanismos, sistemas y controles que detecten hechos asociados de manera integral con la estrategia institucional, la seguridad y privacidad de la información, la seguridad digital, la continuidad de la operación, la gestión ambiental y la seguridad y salud en el trabajo.

El tratamiento o respuesta dada al riesgo se enmarca en las siguientes categorías:

- Aceptar el riesgo: No se adopta ninguna medida que afecte la probabilidad o el impacto del riesgo. La aceptación del riesgo puede ser una opción viable para los riesgos bajos o en aquellos casos donde no sea posible implementar controles efectivos. Sin embargo, en todos los escenarios debe existir un monitoreo continuo del riesgo.

- Reducir el riesgo: Se implementan medidas para disminuir la probabilidad o el impacto del riesgo, o ambos, a través de la aplicación de controles adecuados, la segregación de funciones y la adopción de buenas prácticas en seguridad de la información.

- Evitar el riesgo: Se eliminan o modifican actividades que generan un nivel de riesgo significativo, previniendo su ocurrencia.

- Compartir el riesgo: Se transfiere o comparte parte del riesgo con terceros mediante seguros, acuerdos de servicio o procesos de tercerización. Sin embargo, la responsabilidad final sobre la gestión del riesgo sigue siendo de la institución.

Esta política de administración de riesgos refuerza la seguridad de la información y la continuidad operativa del hospital, asegurando la transparencia, el cumplimiento normativo y la prestación eficiente de los servicios de salud.

7.2.2 IDENTIFICACIÓN DEL RIESGO

La identificación de riesgos en Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de los Servicios en el Hospital Departamental María Inmaculada (HDMI) requiere un análisis integral de los factores que pueden comprometer la seguridad de los activos de información. Este proceso abarca la infraestructura tecnológica, las áreas de trabajo, el entorno físico y digital, y la interacción de los usuarios con los sistemas de información.

Para mitigar riesgos, cada proceso debe contar con un inventario detallado de activos de información y evaluar las amenazas potenciales que puedan afectar la confidencialidad, integridad y disponibilidad de

los datos. Las debilidades en los controles de seguridad pueden ser aprovechadas por actores malintencionados, lo que podría derivar en incidentes que impacten la operatividad del hospital.

Es crucial identificar las amenazas existentes, evaluar las vulnerabilidades y determinar el impacto de su materialización. La recopilación de datos históricos, el análisis de incidentes previos, las evaluaciones técnicas y la consulta con expertos en ciberseguridad son prácticas esenciales para un proceso de identificación efectivo.

7.2.3 VALORACIÓN DEL RIESGO

La valoración del riesgo en el HDMI se llevará a cabo de acuerdo con la metodología definida en la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas del Departamento Administrativo de la Función Pública (DAFP). Este proceso consiste en la evaluación sistemática de la probabilidad e impacto de cada riesgo identificado.

Se aplicará un modelo de análisis basado en la clasificación de riesgos inherentes, determinando sus vulnerabilidades y estableciendo los controles más adecuados para su mitigación. Cada control será evaluado con base en criterios como responsabilidad, periodicidad, efectividad y evidencia de implementación, asegurando que se mantengan alineados con los objetivos de seguridad de la institución.

Para garantizar que los controles sean eficaces, se implementará un sistema de monitoreo continuo que permita ajustar las estrategias de mitigación en función de los cambios en el panorama de amenazas y las necesidades de la institución.

7.2.4 DEFINICIÓN Y APROBACIÓN DE MAPAS DE RIESGOS Y PLANES DE TRATAMIENTO

Una vez finalizado el proceso de identificación y valoración de los riesgos, se procederá a la construcción de los mapas de riesgos, los cuales proporcionarán una visión estructurada de las amenazas y su impacto potencial en la operación del HDMI.

Los líderes de cada proceso serán responsables de revisar y aprobar estos mapas de riesgos, así como los planes de tratamiento diseñados para mitigar aquellos riesgos clasificados como Moderados, Altos o Extremos. Dichos planes incluirán medidas preventivas y correctivas, asegurando la aplicación de controles específicos para reducir la exposición de la organización a vulnerabilidades críticas.

7.2.5 MATERIALIZACIÓN

En caso de materialización de un riesgo, este deberá ser reportado de manera inmediata siguiendo el procedimiento de gestión de incidentes de seguridad y privacidad de la información. Se realizará un análisis posterior para evaluar el impacto real del incidente y determinar las acciones correctivas necesarias.

Si el riesgo materializado no había sido previamente identificado, deberá documentarse para su inclusión en la matriz de riesgos del hospital, garantizando que futuros eventos similares puedan ser gestionados de manera proactiva. Este proceso permitirá fortalecer la postura de seguridad del HDMI y optimizar sus estrategias de mitigación de riesgos.

7.2.6 OPORTUNIDAD DE MEJORA

El Hospital Departamental María Inmaculada (HDMI) debe utilizar la gestión de riesgos no solo como un mecanismo de mitigación, sino también como una oportunidad para optimizar sus procesos institucionales. Cada acción implementada para reducir riesgos puede traducirse en mejoras operativas, fortalecimiento de la resiliencia organizacional y adopción de tecnologías más eficientes.

Esto implica reforzar controles internos, capacitar al personal en mejores prácticas y modernizar herramientas de monitoreo y respuesta ante incidentes. La evaluación continua de los riesgos permitirá anticiparse a posibles problemas, garantizando la eficiencia y seguridad en la prestación de servicios del hospital.

CONTROL DE CAMBIOS		
Versión	**Descripción de cambio**	**Fecha de aprobación**
1.0	Elaboración del plan 2025	

Instructivo para diligenciar el formato
“Plantilla de plan”

Objetivo: Estandarizar la plantilla del documento denominado como plan, sosteniendo uniformidad en todos los documentos de la entidad.

Para el diligenciamiento correcto de la plantilla tenga en cuenta lo siguiente:

Encabezado

Nombre del proceso: Registre solo el nombre completo del proceso al que pertenece el documento, sin que anteceda la palabra **proceso**, en Arial 10 en negrita. Este espacio debe ser sombreado con color verde.

Nombre del documento: Corresponde al nombre que se le sea asignado, a este se le debe anteponer el tipo de documento, por ejemplo, programa. En Arial 12 en negrita.

Código: Registre la identificación alfanumérica del documento, donde se debe registrar la abreviatura del proceso al que corresponda el documento, seguido la abreviatura del tipo de documento y por último el número consecutivo, en Arial 10 en negrita.

Nota: *Si el documento es para elaboración el campo de código será diligenciado por el proceso de mejoramiento continuo.*

Tabla de contenido: El presente tipo de documento debe contar con una tabla de contenido. La cual siempre es recomendable elaborarla de último, respetando su posición dentro del documento.

1. Introducción: Utilice el presente espacio para contextualizar el plan y mencionar lo que está expuesto a continuación, estableciendo la importancia del tema o lo más relevante en el documento, y posteriormente las conclusiones.

2. Objetivo: Registre el propósito central de lo que se espera lograr con el plan en términos de conocimiento; este debe dar inicio con un **solo** verbo infinitivo, por ejemplo: desarrollar, establecer, implementar, entre otros.

3. Términos y definiciones: Relacione los términos y/o definiciones que consideren importante resaltar y que serían una ayuda para el entendimiento del documento. Estos términos, definiciones, siglas y demás deben ir organizados alfabéticamente.

4. Marco normativo o base legal: Registre la normatividad vigente que soporta la información documentada.

5. Responsable: Mencione únicamente el o los cargos de los colaboradores, el nombre del proceso y/o servicio/área que son responsables de adherirse a lo consignado en el documento.

6. Indicadores: Registre los indicadores que considere pertinentes para la medición y seguimiento del plan.

7. Estructura documental: Registre toda la información general, detallada y/o especifica que pretende trasmitir con el documento. A partir de este espacio se pueden incluir todas las herramientas, actividades, imágenes (las cuales deben ir etiquetadas, con su respectiva fuente y relacionadas en la tabla de contenido, en los documentos que aplique) tablas y cualquier otro elemento que consideren importantes para la adecuada comprensión del documento, teniendo en cuenta no extralimitarse con información que redunde o realmente no necesaria para el tipo de documento.