E.S.E. Hospital Santa Mónica

2026

PLAN DE GESTIÓN DEL RIESGO DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

1. INTRODUCCION

La gestión de los riesgos de seguridad y privacidad de la información comprende los procesos de identificación, evaluación, tratamiento, control y seguimiento de los riesgos inherentes a la seguridad y protección de la información.

La finalidad del presente documento es proteger la información institucional, mediante el análisis de las fortalezas y debilidades que puedan afectar tanto los servicios misionales como los de apoyo, garantizando la continuidad, confiabilidad y calidad de los mismos.

De conformidad con lo definido por el Ministerio de Tecnologías de la Información y las Comunicaciones – MINTIC, el Modelo de Seguridad y Privacidad de la Información – MSPI preserva la confidencialidad, integridad, disponibilidad y privacidad de la información, mediante la aplicación del proceso de gestión del riesgo, brindando confianza a las partes interesadas respecto a la adecuada administración de los riesgos de seguridad de la información.

La E.S.E. Hospital Santa Mónica, en cumplimiento de las directrices nacionales y con base en el MSPI, establece que dentro de su Sistema de Gestión de Calidad cuenta con el Manual 04D404-O06 “Manual para la Gestión del Riesgo”, el cual se encuentra fundamentado en la metodología propuesta por el Departamento Administrativo de la Función Pública – DAFP.

El Plan de Gestión del Riesgo de la Seguridad y Privacidad de la Información de la E.S.E. Hospital Santa Mónica se encuentra alineado con el Objetivo de Calidad N.º 4, el cual establece: *“Promover el posicionamiento de la institución a través de la innovación tecnológica, infraestructura adecuada y segura, con un sistema de información integral y oportuno.”*

2. CONTEXTO ESTRATÉGICO

PLATAFORMA ESTRATÉGICA (VER EL DOCUMENTO 02D202 - O16) "PLATAFORMA ESTRATÉGICA INSTITUCIONAL".

3. OBJETIVOS DEL PLAN DE GESTION DEL RIESGO DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

1. **Identificar, evaluar, tratar y monitorear** de manera sistemática y efectiva los riesgos que puedan afectar, de forma positiva o negativa, la **seguridad y privacidad de la información**.

2. **Gestionar y aplicar el tratamiento** a los riesgos identificados que impacten la seguridad y privacidad de la información, de acuerdo con su nivel de criticidad y los lineamientos institucionales.

3. **Controlar y minimizar los riesgos** asociados a los procesos tecnológicos existentes en la **E.S.E. Hospital Santa Mónica**, con el propósito de **salvaguardar los activos de información**, garantizar el adecuado manejo de los medios, el control de accesos y la correcta gestión de usuarios.

4. CONTEXTO ORGANIZACIONAL

La E.S.E Hospital Santa Mónica de Dosquebradas – Risaralda, en su proceso de transición y certificación bajo la NORMA ISO 9001:2015 y los lineamientos dados por el Modelo Integrado de Planeación y Gestión MIPG, tiene documentado e implementado el MANUAL DE GESTION DE LOS RIESGOS, cuyo alcance establece todos los procesos incluidos en el sistema de gestión de calidad de la E.S.E.

Este documento tiene como marco normativo la Ley 87 de 1993 "Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del estado y se dictan otras disposiciones". Modificada parcialmente por la Ley 1474 de 2011.

Por tal motivo la E.S.E Hospital Santa Mónica, definió que para dar cumplimiento al Decreto 612 de 2016, se contará con un solo documento denominado PLAN DE

GESTION DEL RIESGO DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACION, teniendo en cuenta que el TRATAMIENTO DE LOS RIESGOS, se realiza de acuerdo a la metodología antes mencionada.

Todo el proceso de identificación, valoración, tratamiento y monitoreo de los riesgos inherentes a la Seguridad y Privacidad de la Información, se encuentran definidos en el formato 04D404 - F48 IDENTIFICACIÓN, CLASIFICACIÓN Y ANALISIS DE RIESGOS

Es importante aclarar que El PLAN DE GESTION DEL RIESGO DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACION de la E.S.E Hospital Santa Mónica, se encuentra alineado con el Objetivo de Calidad nro. 1, el cual establece "*Brindar una atención humanizada, con enfoque en seguridad del paciente y mejoramiento continuo a través de altos Estándares de calidad, contribuyendo a la satisfacción del usuario*."

5. GESTION DE LOS RIESGOS DE LA SEGURIDAD Y PRIVACIDADDE LA INFORMACION.

El seguimiento y monitoreo a la ejecución de los proyectos planificados en cada vigencia, se realizará a través del Sistema de Gestión de Calidad y Control Interno de la Institución, según la periodicidad establecida en cada uno de ellos.

6. DEFINICION DE CONCEPTOS

Los conceptos relacionados con el tratamiento de los riesgos del SPI, son los mismos manejados en la metodología general y por consiguiente deberán ser consultados en el Manual de Gestión de Riesgos de la E.S.E Hospital Santa Mónica.

Los conceptos a que hace referencia este capítulo hacen referencia a los necesarios para la implementación del SPI.

ACCESO A LA INFORMACIÓN PÚBLICA

Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4).

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 controlar en su calidad de tal.

ARCHIVO

Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3).

AMENAZAS

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

ANÁLISIS DE RIESGO

Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).

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).

AUTORIZACIÓN

Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3).

BASES DE DATOS PERSONALES

Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3). Entiéndase por base de datos, de acuerdo a la Ley de Protección de Datos, cualquier medio electrónico o físico que contenga datos sensibles de los clientes internos y externos de la E.S.E. Hospital Santa Mónica.

CIBERSEGURIDAD

Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).

CIBERESPACIO

Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).

CONTROL

Las políticas, 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. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

DATOS ABIERTOS

Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6).

DATOS PERSONALES

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

DATOS PERSONALES PÚBLICOS

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. (Decreto 1377 de 2013, art 3).

DATOS PERSONALES PRIVADOS

Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h).

DATOS PERSONALES MIXTOS

Para efectos de esta guía es la información que contiene datos personales públicos junto con datos privados o sensibles.

DATOS PERSONALES SENSIBLES

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 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. (Decreto 1377 de 2013, art 3).

DECLARACIÓN DE APLICABILIDAD

Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001. (ISO/IEC 27000).

DERECHO A LA INTIMIDAD

Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).

ENCARGADO DEL TRATAMIENTO DE DATOS

Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del responsable del Tratamiento. (Ley 1581 de 2012, art 3)

GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).

INFORMACIÓN PÚBLICA CLASIFICADA

Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, 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, siempre que se trate de las circunstancias legítimas y necesarias ylos derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).

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 por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)

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).

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 marcolegal vigente.

RESPONSABILIDAD DEMOSTRADA

Conducta desplegada por los responsables o Encargados del tratamiento de datos personales bajo la cual a petición de la Superintendencia de Industria y Comercio deben estar en capacidad de demostrarle a dicho organismo de control que han implementado medidas apropiadas y efectivas para cumplir lo establecidoen la Ley

1581 de 2012 y sus normas reglamentarias.

RESPONSABLE DEL TRATAMIENTO DE DATOS

Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos. (Ley 1581 de 2012, art 3).

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).

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

TITULARES DE LA INFORMACIÓN

Personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3).

TRAZABILIDAD

Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad. (ISO/IEC 27000).

7. RECURSOS

Talento humano: La entidad cuenta con la participación del Gerente, los responsables de proceso y el personal del área de Sistemas de Información, quienes apoyan la implementación, operación y seguimiento de las acciones relacionadas con la seguridad y privacidad de la información.

Recursos tecnológicos: La entidad dispone de infraestructura tecnológica que incluye firewall, equipos de cómputo, servidores y equipos de comunicación, necesarios para la protección de los activos de información y el control de accesos.

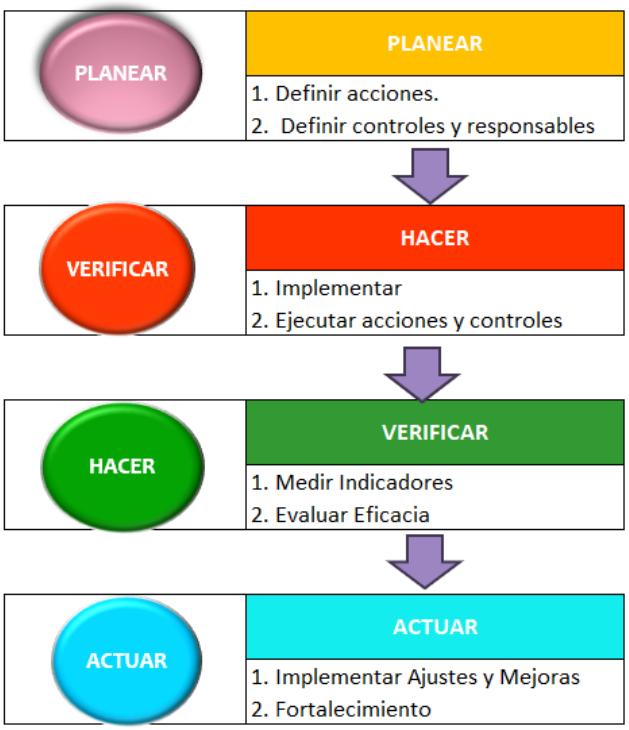
Recursos financieros: Los recursos financieros requeridos para la gestión de la seguridad y privacidad de la información se definen a partir de las etapas de diagnóstico y levantamiento de necesidades y se programan en el Plan Anual de Adquisiciones, de acuerdo con la disponibilidad presupuestal de la entidad.

8. METODOLOGIA DE IMPLEMENTACIÓN

Para la implementación del Plan de Seguridad y Privacidad de la Información (PSPI), la entidad adopta la metodología PHVA (Planear, Hacer, Verificar y Actuar) como enfoque de mejora continua, en concordancia con los lineamientos y directrices emitidos por el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, así como con la normatividad vigente aplicable en materia de seguridad y privacidad de la información.

En este marco, la entidad estructura la implementación del PSPI a través de las siguientes fases, las cuales permiten una gestión sistemática, controlada y evaluable:

1. **Diagnosticar:** Identificación del estado actual de la seguridad y privacidad de la información, análisis de brechas, activos de información, riesgos y cumplimiento de lineamientos del MSPI.
2. **Planear:** Definición de acciones, controles, responsables, cronogramas e indicadores para el tratamiento de los riesgos identificados y el fortalecimiento de la seguridad de la información.
3. **Hacer:** Implementación de las acciones planificadas, ejecución de controles técnicos, administrativos y operativos, y socialización de políticas y procedimientos.
4. **Verificar:** Seguimiento y evaluación del cumplimiento de las acciones definidas, medición de indicadores, revisión de incidentes y verificación de la eficacia de los controles implementados.
5. **Actuar:** Implementación de acciones de mejora continua, ajustes al PSPI y fortalecimiento de los controles, con base en los resultados del seguimiento y las evaluaciones realizadas.


PLANEAR
PLANEAR
1. Definir acciones.
2. Definir controles y responsables
VERIFICAR
HACER
1. Implementar
2. Ejecutar acciones y controles
HACER
VERIFICAR
1. Medir Indicadores
2. Evaluar Eficacia
ACTUAR
ACTUAR
1. Implementar Ajustes y Mejoras
2. Fortalecimiento

9. ACTIVIDADES

- Realizar Diagnóstico
- Levantamiento de los riesgos
- Planteamiento del Plan de Tratamiento de Riegos
- Ajustes a Procesos de TIC del SGC
- Socialización en COMITÉ GOBIERNO EN LINEA, ANTITRAMITES Y PROTECCIÓN DE DATOS, establecido en la entidad a través de la Resolución 196 del 3 de octubre de 2017 y la Resolución 203 de 2022, ““POR MEDIO DE LA CUAL SE ACTUALIZA LAS DISPOSICIONES REFERENTE AL COMITÉ GOBIERNO DIGITAL, ANTITRAMITES Y PROTECCION DE DATOS DE LA E.S.E HOSPITAL SANTA MÓNICA DEL MUNICIPIO DE DOSQUEBRADAS”

10. EJES DE TRABAJO

Los siguientes son los ejes transversales sobre los cuales se deben trabajar elPlan de Gestión de Seguridad y privacidad de la información.

ALTA GERENCIA

Se debe determinarlos procesos y normas que enmarcan la protección de datos personales y considerar las medidas necesarias; así el cómo deben tomarse y cómo mejorarlas. Este enfoque permitirá poner en orden la documentación ygarantizar a los usuarios internos y externos el tratamiento de los datos, la seguridad y la privacidad de los datos que nos confían y que se entregan en su relación con la entidad. Igualmente, la E.S.E evitaría potenciales sanciones que pueden afectar significativamente su patrimonio.

RECURSO HUMANO Y COMUNICACIÓN

Se debe comunicar a los empleados y/o colaboradores de la E.S.E Hospital Santa Mónica, sobre los parámetros que se implementen en materia de protección de datos personales en la entidad, es necesario que comprendan los riesgos y las consecuencias de un uso indebido de los datos.

Para la E.S.E Hospital Santa Mónica, por ser una entidad de salud, cuenta con una condicionante especial en el manejo de historias clínicas y los datos sensiblesde los pacientes. En este sentido se debe garantizar desde Talento Humano y Gestión Comercial, que se comuniquen los lineamientos establecidos al 100% de lasunidades de la entidad.

Para esto se debe tener en cuenta también aquellas condicionantes especiales de las oficinas que hayan diligenciado el INVENTARIO DE BASES DE DATOS y de las cuales dependa su manejo, cuidado y tratamiento. Estas áreas son:

- Epidemiología
- Talento Humano
- Convenios Docencia Servicio
- Seguridad del Paciente
- Cartera
- Jurídica
- Sistemas de Información
- Mantenimiento

PROCESOS INTERNOS

Se deben evaluar e incorporar las directrices para el tratamiento de los datos en las áreas y procesos a los que les corresponda. Para esto se analizará su impactoy requerimientos, cada dueño de proceso deberá ajustar sus procesos y su documentación, de acuerdo a los lineamientos del SGC.

Este eje está muy relacionado con la aplicación de las normas sobre la administración de archivos tanto físicos como automatizados, que genera un gran riesgo de pérdida, adulteración, circulación no permitida, acceso no autorizado de terceros, entre otros aspectos.

Por ello debe evaluar los mecanismos para garantizar los derechos de los Titulares de los datos en el ciclo vital de la información. El documento principal que evidencia el cumplimiento de este eje lo aportan todos los Consentimientos de los Titulares de Información, contenidos y descritos en las bases de datosinstitucionales.

DATOS PERSONALES

Se debe asegurar el control y la calidad de los datos personales que se almacena en las bases de datos. Para ello, debe identificar donde y quien administra al interior de la compañía las bases de datos que contienen información personal, el tipo de dato que maneja, quienes son sus Titulares, para qué los utiliza, cuantos datos tiene y considere cómo puede interactuar con los Titulares y/o terceros. Esta condición es clave para ofrecer la

transparencia y confianza, que exige el marco legal en cuanto al PSPI.

Se debe garantizar y comprender el flujo interno y externo de dicha información considerando a través de qué canales se obtiene, donde se procesa, el uso que sele da y a quién se transmite y/o transfiere.

De esta forma la entidad debe garantizar los Consentimientos Institucionales y/o Personales necesarios para dar cumplimiento a la norma.

SEGURIDAD DE INFORMACIÓN

El último eje establece el implementar y/o mejorar la Protección de la información garantizando la confidencialidad, disponibilidad e integridad de datos. Se deben implementar medidas preventivas desde cada proceso; tanto asistencial como de apoyo y gerencial; y los sistemas tecnológicos con el fin de suministrar herramientas eficaces para la gestión interna y defienda a la entidad de incidentes o ataques de terceros.

11. IMPLEMENTACIÓN

De acuerdo a lo definido en los capítulos 8 y 9, los siguientes son los puntos a desarrollar y los plazos de implementación.

- Realizar Diagnóstico
- Levantamiento de los riesgos
- Planteamiento del Plan de Tratamiento de Riegos
- Ajustes a Procesos de TIC del SGC
- Socialización en COMITÉ GOBIERNO EN LINE, ANTITRAMITES Y PROTECCIÓN DE DATOS, establecido en la entidad a través de la Resolución 196 del 3 de octubre de 2017 y la Resolución 203 de 2022, ““POR MEDIO DE LA CUAL SE ACTUALIZA LAS DISPOSICIONES REFERENTE AL COMITÉ GOBIERNO DIGITAL, ANTITRAMITES Y PROTECCION DE DATOS DE LA E.S.E HOSPITAL SANTA MÓNICA DEL MUNICIPIO DE DOSQUEBRADAS”

ACIVIDAD	VIGENCIA 2026			
	Primer Trimestre	Segundo Trimestre	Tercer Trimestre	Cuarto Trimestre
ACTUALIZAR DIAGNÓSTICO				
ACTUALIZAR MAPA DE LOS RIESGOS				
Planteamiento del Plan de Tratamiento de Riegos				
Ajustes a Procesos de TIC del SGC				
Socialización en COMITÉ GOBIERNO EN LINEA, ANTITRAMITES Y PROTECCIÓN DE DATOS				

12. SEGUIMIENTO DEL PLAN

El seguimiento y monitoreo a la ejecución de los proyectos planificados encada vigencia, se realizará a través del Sistema de Gestión de Calidad y la oficina de Planeación, según la periodicidad establecida en cada unode ellos.

13. APROBACIÓN Y PUBLICACIÓN

El **PLAN DE GESTION DEL RIESGO DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACION**- se aprobará por el Comité de Gestión y Desempeño; una vez aprobado se incluirá en el Sistema de Gestión de Calidad y su posterior publicación en la página Web de la entidad.

14. WEBGRAFIA

[Citado el 27 de Julio de 2018] Disponible en Internet: <.https://www.mintic.gov.co/gestionti/615/articles-5482_Guia_Seguridad_informacion_Mypimes.pdf >

E.S.E. Hospital Santa Mónica	NOMBRE **ACTIVIDADES PLANES INSTITUCIONALES**		CÓDIGO **02D202 - F12**
			VERSIÓN **2.0**
	TIPO DOCUMENTO **FORMATO**	ÁREA RESPONSABLE **GERENCIA**	FECHA DE VIGENCIA **13/12/2024**
ÁREA RESPONSABLE	SISTEMAS DE INFORMACION Y GESTION DOCUMENTAL		
NOMBRE PLAN INSTITUCIONAL	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN		

ACTIVIDAD	RESPONSABLE	FECHA INICIAL	FECHA FINAL	INDICADOR
1. Actualizar Diagnóstico	Coordinadora Sistemas de Información y Gestión Documental	Primer Trimestre 2026	Primer Trimestre 2026	Diagnóstico Actualizado
2. Levantamiento De Los Riesgos	Coordinadora Sistemas de Información y Gestión Documental	Segundo Semestre de la Vigencia 2026	Segundo Semestre de la Vigencia 2026	Riesgos identificados en cumplimiento a lo establecido en el SGC
3. Planteamiento Del Plan De Tratamiento De Riegos	Coordinadora Sistemas de Información y Gestión Documental	Segundo Semestre de la Vigencia 2026	Segundo Semestre de la Vigencia 2026	Plan de Tratamiento de los riesgos realizado
4. Ajustes a Procesos de TIC del SGC	Coordinadora Sistemas de Información y Gestión Documental	Diciembre de 2026	Diciembre de 2026	Proceso actualizado en el SGC
5. Socialización En Comité Gobierno Digital , Antitramites Y Proteccion De Datos	Coordinadora Sistemas de Información y Gestión Documental	Diciembre de 2026	Diciembre de 2026	Comités Realizados