

Resolución 040 de 2025

(Enero 28 - 2025)

"Mediante la cual se adoptan, integran y se ordena la publicación de los Planes Institucionales y Estratégicos de la ESE Hospital Alcides Jiménez para la vigencia 2025"

EL GERENTE DE LA ESE HOSPITAL ALCIDES JIMENEZ del Municipio de Puerto Caicedo (Putumayo), en ejercicio de sus facultades legales en especial las conferidas por la Ley 100 de 1993, ley 1438 de 2011 y el Decreto Departamental No. 00102 del 27 de marzo de 2024, y

CONSIDERANDO:

Que la Ley 1474 de 2011 en su artículo 74 establece que toda entidad del estado a más tardar el 31 de enero de cada vigencia deberá publicar en su respectiva página web el plan de acción para el año siguiente, el cual comprende objetivos, estrategias, las metas, los responsables.

Que la Circular Externa de la Superintendencia de Salud N° 009 de 2015 establece que el director o gerente de la Empresa Social del Estado deberá presentar la información requerida en los numerales 9 y 10, que se debe presentar el Plan de Acción y los avances de ejecución a los que se refiere el artículo N° 74 de la Ley 1474 de 2011.

Que a su vez el Decreto Nacional 1083 de 2015, Decreto Único Reglamentario del Sector de Función Pública, reglamentado por el Decreto 612 de 2018, indica en su artículo 2.2.22.3.14. Y siguientes que las entidades del Estado, de acuerdo con el ámbito de aplicación del Modelo Integrado de Planeación y Gestión y al Plan de Acción de que trata el artículo 74 de la Ley 1474 de 2011; deberán integrar, adoptar y publicar en su respectiva página web a 31 de enero los siguientes planes: 1. Plan Institucional de archivos, 2. Plan Anual de Vacantes; 3. Plan de Previsión del Talento Humano; 4. Plan Estratégico de Talento Humano; 5. Plan de Incentivos Institucionales; 6. Plan anual de Adquisiciones; 7. Plan Institucional de Capacitación; 8. Plan de Trabajo del Sistema de Seguridad y Salud en el Trabajo; 9. Plan Anticorrupción y Atención al

Ciudadano; 10. Plan Estratégico de Tecnologías de la Información y Comunicaciones PETI; 11. Plan de Riesgos de Seguridad y Privacidad de la Información; 12. Plan de Seguridad y Privacidad de la Información.

Que a la fecha actual están debidamente formulados y presentados los diferentes Planes Institucionales y Planes Estratégicos para la vigencia 2024 por cada uno de los líderes de proceso y de apoyo, indicados en el numeral precedente.

Que mediante Resolución 041 de 2021 "Por medio de la cual se actualiza el Comité Institucional de Gestión y Desempeño de la Empresa Social del Estado Hospital Alcides Jiménez" se determinó la conformación, las funciones, los deberes, la secretaría técnica, las convocatorias, el quorum y las actas del Comité Institucional de Gestión y Desempeño que ha avalado la formulación de estos planes y programas según cada área.

Que por lo anteriormente expuesto el Gerente de La Empresa Social del Estado Hospital Alcides Jiménez.

RESUELVE

ARTÍCULO PRIMERO: Adóptense, Intégrense y publíquense mediante la presente Resolución única, los Planes y programas Institucionales y Planes Estratégicos relacionados a continuación:

1. Plan de Acción Institucional o Plan Operativo anual
2. Plan Institucional de Archivo
3. Plan Anual de Vacantes
4. Plan de Previsión del Talento Humano
5. Plan Estratégico de Talento Humano
6. Plan de Incentivos Institucionales
7. Plan anual de Adquisiciones
8. Plan Institucional de Capacitación
9. Plan de Trabajo del Sistema de Seguridad y Salud en el Trabajo
10. Plan Anticorrupción y Atención al ciudadano
11. Plan Estratégico de Tecnologías de la Información y Comunicaciones PETI
12. Plan de Riesgos de Seguridad y Privacidad de la Información
13. Plan de Seguridad y Privacidad de la Información



E.S.E HOSPITAL ALCIDES JIMÉNEZ
NIT. 846.001.669-0

FORMATO DE RESOLUCIONES INSTITUCIONAL
Código: AD-PL-002-F-007
Versión: 2

PARÁGRAFO 1: Los presentes planes y programas rigen para la vigencia 2025.

ARTÍCULO SEGUNDO: VIGENCIA: La presente Resolución rige a partir de la fecha de expedición.

PUBLÍQUESE Y CUMPLASE

Dada en la E.S.E. Hospital Alcides Jiménez del Municipio de Puerto Caicedo Putumayo, a los veintiocho (28) días del mes de enero de Dos mil veinticinco (2025).

ESTEBAN LOPEZ BURBANO
Gerente
E.S.E Hospital Alcides Jiménez

<i>Elaboró</i>	<i>Edwin Jesus Insuasty Insuasty</i>	<i>Profesional de Planeación</i>	
<i>Revisó</i>	<i>Diego Fernando Narváez Solarte</i>	<i>Asesor Jurídico</i>	

	E.S.E HOSPITAL ALCIDES JIMENEZ NIT. 846.001.669-0	VERSIÓN: 02	CÓDIGO: AD-PL- 002
	PLAN DE TRATAMIENTO DE RIESGO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2025	FECHA DE ACTUALIZACIÓN 17 de Enero de 2025	
		PAGINA: 1 DE 15	

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN - 2025



Esteban López Burbano
 Gerente E.S.E. H.A.J.

PUERTO CAICEDO – PUTUMAYO

ELABORADO POR: RUBÉN DARÍO GUZMÁN VALLEJO	REVISADO POR: BYRON STEVEN AGUDELO	APROBADO POR: ESTEBAN LÓPEZ BURBANO
CARGO: ING. DE SISTEMAS	CARGO: Subgerente	CARGO: Gerente
FECHA: 17 de Enero de 2025	FECHA: 17 de Enero de 2025	FECHA: 17 de Enero de 2025

"Documento controlado del Sistema de Gestión de Calidad de la E.S.E Hospital Alcides Jiménez. Su Reproducción no es válida sin autorización".

	E.S.E HOSPITAL ALCIDES JIMENEZ NIT. 846.001.669-0	VERSIÓN: 02	CÓDIGO: AD-PL- 002
	PLAN DE TRATAMIENTO DE RIESGO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2025	FECHA DE ACTUALIZACIÓN 17 de Enero de 2025	
		PAGINA: 2 DE 15	

RESUMEN EJECUTIVO

Mediante la definición del Plan de Tratamiento de Riesgos la E.S.E. HOSPITAL ALCIDES JIMENEZ se busca mitigar los riesgos presentes en el análisis de riesgos (Pérdida de la Confidencialidad, Pérdida de Integridad y Pérdida de Disponibilidad), en la información digital, evitando aquellas situaciones que impidan el logro Estratégicos del Hospital.

El Plan de Tratamiento de Riesgo se define con el fin de evaluar las posibles acciones que se deben tomar para mitigar los riesgos existentes en los activos de información del Hospital, estas acciones son organizadas en forma de medias de seguridad denominados controles, y para cada una de ellas se define el nombre de la medida, objetivo, justificación, responsable de la medida y su prioridad.

Las anteriores medidas se definen teniendo en cuenta la información del análisis de riesgos, sobre la plataforma informática y las necesidades del Proceso de Gestión de la Infraestructura de las TIC del Hospital, en cuanto a la seguridad de la información y proporciona las herramientas necesarias para definir cada una de las características de las medidas y la definición de los pasos a seguir para su ejecución.

ELABORADO POR: RUBÉN DARÍO GUZMÁN VALLEJO	REVISADO POR: BYRON STEVEN AGUDELO	APROBADO POR: ESTEBAN LÓPEZ BURBANO
CARGO: ING. DE SISTEMAS	CARGO: Subgerente	CARGO: Gerente
FECHA: 17 de Enero de 2025	FECHA: 17 de Enero de 2025	FECHA: 17 de Enero de 2025

"Documento controlado del Sistema de Gestión de Calidad de la E.S.E Hospital Alcides Jiménez. Su Reproducción no es válida sin autorización".



INTRODUCCIÓN

El plan de tratamiento de riesgos de Seguridad y Privacidad de la información, Seguridad Digital en la E.S.E. HOSPITAL ALCIDES JIMENEZ, se basa en una orientación estratégica que requiere el desarrollo de una cultura de carácter preventivo en la entidad, de manera que, al comprender el concepto de riesgo, así como el contexto, a través de este instrumento se planean las acciones que reduzcan la afectación a la entidad en caso de materialización de estos, adicional se busca desarrollar estrategias para la identificación, análisis, tratamiento, evaluación y monitoreo de dichos riesgos con mayor objetividad, dando a conocer aquellas situaciones que pueden comprometer el cumplimiento de los objetivos trazados en el mundo en el Entorno Digital.

Lo anterior dando cumplimiento a la normativa establecida por el estado colombiano, CONPES 3854 de 2016, Modelo de Seguridad y Privacidad de MINTIC y lo establecido en el decreto 1008 de 14 de junio 2018, adoptando las buenas prácticas y los lineamientos del estándar ISO 27001:2012, alineado con ISO 31000:2018 y la guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital - Versión 4 emitida por el Departamento Administrativo de la Funciona Pública y aquellas que él Hospital defina.



Ilustración 1. Elementos básicos de la gestión de riesgos de seguridad y privacidad de la información

ELABORADO POR: RUBÉN DARÍO GUZMÁN VALLEJO	REVISADO POR: BYRON STEVEN AGUDELO	APROBADO POR: ESTEBAN LÓPEZ BURBANO
CARGO: ING. DE SISTEMAS	CARGO: Subgerente	CARGO: Gerente
FECHA: 17 de Enero de 2025	FECHA: 17 de Enero de 2025	FECHA: 17 de Enero de 2025

	E.S.E HOSPITAL ALCIDES JIMENEZ NIT. 846.001.669-0	VERSIÓN: 02	CÓDIGO: AD-PL- 002
	PLAN DE TRATAMIENTO DE RIESGO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2025	FECHA DE ACTUALIZACIÓN 17 de Enero de 2025	
		PAGINA: 4 DE 15	

DEFINICIONES

A continuación, se listan algunos términos y definiciones de términos que se utilizarán durante el desarrollo de la gestión de riesgos de seguridad de la información, en beneficio de unificar criterios dentro de la Agencia.

Administración del riesgo: Conjunto de elementos de control que al interrelacionarse brindan a la entidad la capacidad para emprender las acciones necesarias que le permitan el manejo de los eventos que puedan afectar negativamente el logro de los objetivos institucionales y protegerla de los efectos ocasionados por su ocurrencia.

Activo de Información: En relación con la seguridad de la información, se refiere a cualquier información o elemento de valor para los procesos de la Organización.

Análisis de riesgos: Es un método sistemático de recopilación, evaluación, registro y difusión de información necesaria para formular recomendaciones orientadas a la adopción de una posición o medidas en respuesta a un peligro determinado.

Amenaza: Es la causa potencial de una situación de incidente y no deseada por la organización

Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

Consecuencia: Resultado de un evento que afecta los objetivos.

Criterios del riesgo: Términos de referencia frente a los cuales la importancia de un riesgo se evalúa.

Control: Medida que modifica el riesgo.

Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

Evaluación de riesgos: Proceso de comparación de los resultados del análisis del riesgo con los criterios del riesgo, para determinar si el riesgo, su magnitud o ambos son aceptables o tolerables.

Evento: Un incidente o situación, que ocurre en un lugar particular durante un

ELABORADO POR: RUBÉN DARÍO GUZMÁN VALLEJO	REVISADO POR: BYRON STEVEN AGUDELO	APROBADO POR: ESTEBAN LÓPEZ BURBANO
CARGO: ING. DE SISTEMAS	CARGO: Subgerente	CARGO: Gerente
FECHA: 17 de Enero de 2025	FECHA: 17 de Enero de 2025	FECHA: 17 de Enero de 2025

"Documento controlado del Sistema de Gestión de Calidad de la E.S.E Hospital Alcides Jiménez. Su Reproducción no es válida sin autorización".

	E.S.E HOSPITAL ALCIDES JIMENEZ NIT. 846.001.669-0	VERSIÓN: 02	CÓDIGO: AD-PL- 002
	PLAN DE TRATAMIENTO DE RIESGO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2025	FECHA DE ACTUALIZACIÓN 17 de Enero de 2025	
		PAGINA: 5 DE 15	

intervalo de tiempo específico.

Estimación del riesgo. Proceso para asignar valores a la probabilidad y las consecuencias de un riesgo.

Evitación del riesgo: Decisión de no involucrarse en una situación de riesgo o tomar acción para retirarse de dicha situación.

Factores de Riesgo: Situaciones, manifestaciones o características medibles u observables asociadas a un proceso que generan la presencia de riesgo o tienden a aumentar la exposición, pueden ser internos o externos a la entidad.

Gestión del riesgo: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo, se compone de la evaluación y el tratamiento de riesgos.

Identificación del riesgo: Proceso para encontrar, enumerar y caracterizar los elementos de riesgo.

Incidente de seguridad de la información: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información (Confidencialidad, Integridad y Disponibilidad).

Integridad: Propiedad de la información relativa a su exactitud y completitud.

Impacto. Cambio adverso en el nivel de los objetivos del negocio logrados.

Nivel de riesgo: Magnitud de un riesgo o de una combinación de riesgos, expresada en términos de la combinación de las consecuencias y su posibilidad.

Matriz de riesgos: Instrumento utilizado para ubicar los riesgos en una determinada zona de riesgo según la calificación cualitativa de la probabilidad de ocurrencia y del impacto de un riesgo.

Monitoreo: Mesa de trabajo anual, la cual tiene como finalidad, revisar, actualizar o redefinir los riesgos de seguridad de la información en cada uno de los procesos, partiendo del resultado de los seguimientos y/o hallazgos de los entes de control o las diferentes auditorías de los sistemas integrados de gestión.

ELABORADO POR: RUBÉN DARÍO GUZMÁN VALLEJO	REVISADO POR: BYRON STEVEN AGUDELO	APROBADO POR: ESTEBAN LÓPEZ BURBANO
CARGO: ING. DE SISTEMAS	CARGO: Subgerente	CARGO: Gerente
FECHA: 17 de Enero de 2025	FECHA: 17 de Enero de 2025	FECHA: 17 de Enero de 2025

"Documento controlado del Sistema de Gestión de Calidad de la E.S.E Hospital Alcides Jiménez. Su Reproducción no es válida sin autorización".

	E.S.E HOSPITAL ALCIDES JIMENEZ NIT. 846.001.669-0	VERSIÓN: 02	CÓDIGO: AD-PL- 002
	PLAN DE TRATAMIENTO DE RIESGO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2025	FECHA DE ACTUALIZACIÓN 17 de Enero de 2025	
		PAGINA: 6 DE 15	

Propietario del riesgo: Persona o entidad con la responsabilidad de rendir cuentas y la autoridad para gestionar un riesgo.

Proceso: Conjunto de actividades interrelacionadas o que interactúan para transformar una entrada en salida.

Riesgo Inherente: Es el nivel de riesgo propio de la actividad, sin tener en cuenta el efecto de los controles.

Riesgo Residual: El riesgo que permanece tras el tratamiento del riesgo o nivel resultante del riesgo después de aplicar los controles.

Riesgo: Efecto de la incertidumbre sobre los objetivos.

Riesgo en la seguridad de la información: Potencial de que una amenaza determinada explote las vulnerabilidades de los activos o grupos de activos causando así daño a la organización.

Reducción del riesgo: Acciones que se toman para disminuir la probabilidad las consecuencias negativas, o ambas, asociadas con un riesgo.

Retención del riesgo: Aceptación de la pérdida o ganancia proveniente de un riesgo particular

Seguimiento: Mesa de trabajo semestral, en el cual se revisa el cumplimiento del plan de acción, indicadores y metas de riesgo y se valida la aplicación n de los controles de seguridad de la información sobre cada uno de los procesos.

Tratamiento del Riesgo: Proceso para modificar el riesgo" (Icontec Internacional, 2011).

Valoración del Riesgo: Proceso global de identificación del riesgo, análisis del riesgo y evaluación de los riesgos.

Vulnerabilidad: Es aquella debilidad de un activo o grupo de activos de información

Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información.

MSPI: Modelo de Seguridad y privacidad.

ELABORADO POR: RUBÉN DARÍO GUZMÁN VALLEJO	REVISADO POR: BYRON STEVEN AGUDELO	APROBADO POR: ESTEBAN LÓPEZ BURBANO
CARGO: ING. DE SISTEMAS	CARGO: Subgerente	CARGO: Gerente
FECHA: 17 de Enero de 2025	FECHA: 17 de Enero de 2025	FECHA: 17 de Enero de 2025

"Documento controlado del Sistema de Gestión de Calidad de la E.S.E Hospital Alcides Jiménez. Su Reproducción no es válida sin autorización".

	E.S.E HOSPITAL ALCIDES JIMENEZ NIT. 846.001.669-0	VERSIÓN: 02	CÓDIGO: AD-PL- 002
	PLAN DE TRATAMIENTO DE RIESGO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2025	FECHA DE ACTUALIZACIÓN 17 de Enero de 2025	
		PAGINA: 7 DE 15	

Riesgos de seguridad digital: posibilidad de combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales. Incluye aspectos relacionados con el ambiente físico, digital y las personas.

OBJETIVOS

La gestión de riesgos constituye una estrategia con el propósito de definir y aplicar los lineamientos para tratar de manera integral los riesgos de Seguridad Digital que el Hospital General de Medellín pueda estar expuesto, y de esta manera alcanzar el plan estratégico, los objetivos, la misión y la visión institucional, protegiendo y preservando la integridad, confidencialidad y disponibilidad y de la información, los principales Objetivos de esta gestión son:

1. Cumplir con los requisitos legales y reglamentarios pertinentes a la legislación colombiana en materia de seguridad de la información.
2. Gestionar riesgos de Seguridad y Privacidad de la información, Seguridad Digital, de acuerdo con los contextos establecidos en la Entidad.
3. Fortalecer y apropiar conocimiento referente a la gestión de riesgos Seguridad y Privacidad de la información, Seguridad Digital.
4. Alinear el Plan de Desarrollo Municipal, Plan de Desarrollo del Hospital General de Medellín y Plan de Seguridad y Privacidad del Hospital con este plan de tratamiento de riesgos.
5. Emplear un enfoque de sistemas para planificar, implementar, monitorizar y gestionar los riesgos de seguridad digital.

ALCANCE

Con el propósito de realizar una eficiente gestión de riesgos de Seguridad Digital en la E.S.E. HOSPITAL ALCIDES JIMENEZ, esta actividad se debe realizar integrando los procesos de la entidad con este plan, mediante el uso de buenas prácticas y lineamientos nacionales, y locales, con el propósito que ello contribuya a la toma de

ELABORADO POR: RUBÉN DARÍO GUZMÁN VALLEJO	REVISADO POR: BYRON STEVEN AGUDELO	APROBADO POR: ESTEBAN LÓPEZ BURBANO
CARGO: ING. DE SISTEMAS	CARGO: Subgerente	CARGO: Gerente
FECHA: 17 de Enero de 2025	FECHA: 17 de Enero de 2025	FECHA: 17 de Enero de 2025

"Documento controlado del Sistema de Gestión de Calidad de la E.S.E Hospital Alcides Jiménez. Su Reproducción no es válida sin autorización".

	E.S.E HOSPITAL ALCIDES JIMENEZ NIT. 846.001.669-0	VERSIÓN: 02	CÓDIGO: AD-PL- 002
	PLAN DE TRATAMIENTO DE RIESGO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2025	FECHA DE ACTUALIZACIÓN 17 de Enero de 2025	
		PAGINA: 8 DE 15	

decisiones y prevenir incidentes que puedan afectar el logro de los objetivos.

A partir de lo anterior se definen los lineamientos mediante una guía de para la gestión de riesgos de Seguridad Digital, para el tratamiento de los riesgos asociados a la información que es soportada por componentes tecnológicos en el entorno digital.

El Plan de Tratamiento de Riesgo tendrá en cuenta los riesgos que superen el NRA (nivel de riesgo aceptable), de igual manera se deben monitorear los riesgos residuales periódicamente según la planeación de la entidad.

MARCO REFERENCIAL

POLÍTICA DE ADMINISTRACION DE RIESGOS

La E.S.E. HOSPITAL ALCIDES JIMENEZ a través de su Modelo de Seguridad y Privacidad, se compromete a mantener una cultura de la gestión del riesgo digital, con un enfoque basado en los riesgos de seguridad digital en los procesos y proyectos luchando continuamente contra la corrupción, mediante mecanismos, sistemas y controles enfocados a la prevención y detección de hechos asociados a este fenómeno y fortaleciendo las medidas de control y la eficiencia a lo largo del ciclo de vida del proyecto para optimizar de manera continua y oportuna la respuesta a los riesgos además de los de seguridad y privacidad de la Información y Seguridad Digital de manera Integral.

La política identifica las opciones para tratar y manejar los riesgos basados en su valoración, permiten tomar decisiones adecuadas y fijar los lineamientos para administración de los mismos; a su vez, transmiten la posición de la dirección y establecen las guías de acción necesarias a todos los colaboradores del Hospital.

Se deben tener en cuentas algunas de las siguientes opciones, las cuales pueden considerarse independientemente, interrelacionadas o en conjunto:

- **Evitar:** es eliminar la probabilidad de ocurrencia o disminuir totalmente el impacto, lo que requiere la eliminación de la actividad o fuente de riesgo del

ELABORADO POR: RUBÉN DARÍO GUZMÁN VALLEJO	REVISADO POR: BYRON STEVEN AGUDELO	APROBADO POR: ESTEBAN LÓPEZ BURBANO
CARGO: ING. DE SISTEMAS	CARGO: Subgerente	CARGO: Gerente
FECHA: 17 de Enero de 2025	FECHA: 17 de Enero de 2025	FECHA: 17 de Enero de 2025

	E.S.E HOSPITAL ALCIDES JIMENEZ NIT. 846.001.669-0	VERSIÓN: 02	CÓDIGO: AD-PL- 002
	PLAN DE TRATAMIENTO DE RIESGO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2025	FECHA DE ACTUALIZACIÓN 17 de Enero de 2025	
		PAGINA: 9 DE 15	

activo, eliminar la exposición y su expresión máxima es dejar una actividad. Por ejemplo, para evitar pérdida de archivos se retiran los permisos de acceso.

- **Prevenir:** corresponde al área de planeación, esto es, planear estrategias conducentes a que el evento no ocurra o que disminuya su probabilidad. Un ejemplo de ello son las inspecciones el mantenimiento preventivo, las políticas de seguridad o las revisiones periódicas a los procesos.
- **Reducir o mitigar:** corresponde a la protección en el momento en que se presenta el riesgo se encuentra en esta categoría los planes de emergencia planes de contingencia equipos de protección personal, ambiental, de acceso mantener copias de respaldo
- **Dispersar:** es dividir una actividad en diferentes componentes operativos, de manera que las actividades no se concentren en un mismo sitio o bajo una sola responsabilidad. Este es el caso de los contratos de suministro de partes, la ubicación de nodos, plantas alternas, equipos paralelos, contratar obras por tramos
- **Compartir:** es involucrar a un tercero para que responda en todo o en parte por el riesgo que genera una actividad. Dentro de los mecanismos de transferencia se encuentran los siguientes: contratos de seguro, transferencia explícita por medio de cláusulas contractuales, derivados financieros.

Los riesgos detectados deberán ser analizados de tal forma que se pueda determinar cuál va a ser su tratamiento. Así mismo, teniendo en cuenta lo expuesto en la Guía de Gestión de Riesgos de Seguridad y Privacidad de la Información, las *"(...) no se debe olvidar que dentro del análisis de los controles se debe tener en cuenta al dueño del riesgo (dueño del proceso), ya que la definición de los controles es el resultado de los análisis realizados a través del seguimiento y aplicación de los pasos descritos anteriormente en el tratamiento del riesgo y los cuales deben tener el concurso de todos los interesados"*(...).

ELABORADO POR: RUBÉN DARÍO GUZMÁN VALLEJO	REVISADO POR: BYRON STEVEN AGUDELO	APROBADO POR: ESTEBAN LÓPEZ BURBANO
CARGO: ING. DE SISTEMAS	CARGO: Subgerente	CARGO: Gerente
FECHA: 17 de Enero de 2025	FECHA: 17 de Enero de 2025	FECHA: 17 de Enero de 2025

"Documento controlado del Sistema de Gestión de Calidad de la E.S.E Hospital Alcides Jiménez. Su Reproducción no es válida sin autorización".

	E.S.E HOSPITAL ALCIDES JIMENEZ NIT. 846.001.669-0	VERSIÓN: 02	CÓDIGO: AD-PL- 002
	PLAN DE TRATAMIENTO DE RIESGO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2025	FECHA DE ACTUALIZACIÓN 17 de Enero de 2025	
		PAGINA: 10 DE 15	

METODOLOGÍA

Mediante un

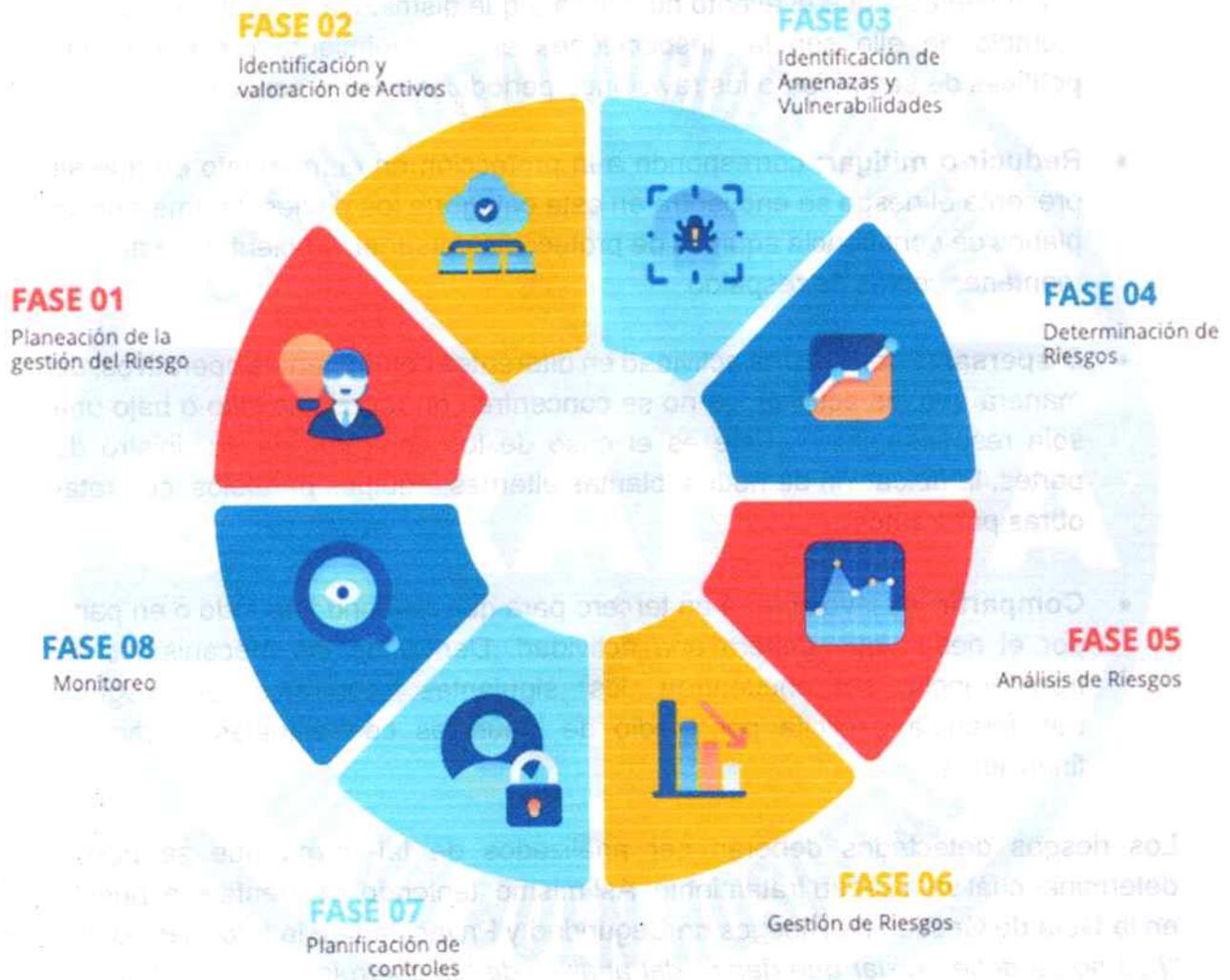


Ilustración 2. Fases de Implementación

ELABORADO POR: RUBÉN DARÍO GUZMÁN VALLEJO	REVISADO POR: BYRON STEVEN AGUDELO	APROBADO POR: ESTEBAN LÓPEZ BURBANO
CARGO: ING. DE SISTEMAS	CARGO: Subgerente	CARGO: Gerente
FECHA: 17 de Enero de 2025	FECHA: 17 de Enero de 2025	FECHA: 17 de Enero de 2025

"Documento controlado del Sistema de Gestión de Calidad de la E.S.E Hospital Alcides Jiménez. Su Reproducción no es válida sin autorización".



E.S.E HOSPITAL ALCIDES JIMENEZ
NIT. 846.001.669-0

VERSIÓN:
02

CÓDIGO: AD-PL-
002

**PLAN DE TRATAMIENTO DE RIESGO DE
SEGURIDAD Y PRIVACIDAD DE LA
INFORMACIÓN 2025**

FECHA DE ACTUALIZACIÓN
17 de Enero de 2025

PAGINA: 11 DE 15

Fase	Actividades	Responsable	Fecha Inicio	Fecha Fin
Fase 1 Planeación de la gestión del Riesgo	Revisar y ajustar metodología para la gestión de Riesgo de Seguridad Digital acorde a las necesidades del Hospital Alcides Jimenez. Revisión Guía de Gestión de Riesgos de Seguridad Digital Hospital Alcides Jimenez.	Área Sistemas	Enero	Abril
Fase 2 Identificación y valoración de Activos	Identificación/Actualización de Activo de Información. Clasificación de Activos de Información. Valoración de Activos de Información.	Área Sistemas	Mayo	Julio
Fase 3 Identificación de Amenazas y Vulnerabilidades	Identificación de Amenazas y Vulnerabilidades.	Área Sistemas	Agosto	Octubre
Fase 4 Determinación de Riesgos	Determinación del Impacto de las amenazas por activo Determinación de Probabilidad de Ocurrencia	Área Sistemas	Noviembre	Diciembre
Fase 5 Análisis de Riesgos	Cálculo de Riesgos Identificación de Riesgos superiores al NRA	Área Sistemas	Noviembre	Diciembre
Fase 6 Gestión de Riesgos	Determinación de Controles Tratamiento de Riesgos Diseño de controles Priorización de Controles	Área Sistemas	Noviembre	Diciembre

ELABORADO POR: RUBÉN DARÍO GUZMÁN VALLEJO	REVISADO POR: BYRON STEVEN AGUDELO	APROBADO POR: ESTEBAN LÓPEZ BURBANO
CARGO: ING. DE SISTEMAS	CARGO: Subgerente	CARGO: Gerente
FECHA: 17 de Enero de 2025	FECHA: 17 de Enero de 2025	FECHA: 17 de Enero de 2025

"Documento controlado del Sistema de Gestión de Calidad de la E.S.E Hospital Alcides Jiménez. Su Reproducción no es válida sin autorización".

	E.S.E HOSPITAL ALCIDES JIMENEZ NIT. 846.001.669-0	VERSIÓN: 02	CÓDIGO: AD-PL- 002
	PLAN DE TRATAMIENTO DE RIESGO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2025	FECHA DE ACTUALIZACIÓN 17 de Enero de 2025	
		PAGINA: 12 DE 15	

Fase 7 Planificación de controles	Implementación de Controles que no requieren recursos. Planificación de Controles (Presupuesto próximo año).	Área Sistemas y áreas responsables	Noviembre	Diciembre
Fase 8 Monitoreo	Medición de la eficacia de los controles	Área Sistemas y Áreas responsables	Permanente Trimestral	N/A

NOTA: Los controles seleccionados serán confrontados con los establecidos en el Anexo A del estándar ISO 27001:2022 como pilar fundamental del Modelo de Seguridad y Privacidad del Hospital General.

DESARROLLO METODOLÓGICO

En la figura siguiente se presenta el modelo de gestión de riesgos de seguridad de la información basada tanto en la norma ISO/IEC 31000 como en la ISO 27005 para la adecuada administración de riesgos en la seguridad de la información; los elementos que lo componen son:

ELABORADO POR: RUBÉN DARÍO GUZMÁN VALLEJO	REVISADO POR: BYRON STEVEN AGUDELO	APROBADO POR: ESTEBAN LÓPEZ BURBANO
CARGO: ING. DE SISTEMAS	CARGO: Subgerente	CARGO: Gerente
FECHA: 17 de Enero de 2025	FECHA: 17 de Enero de 2025	FECHA: 17 de Enero de 2025

"Documento controlado del Sistema de Gestión de Calidad de la E.S.E Hospital Alcides Jiménez. Su Reproducción no es válida sin autorización".

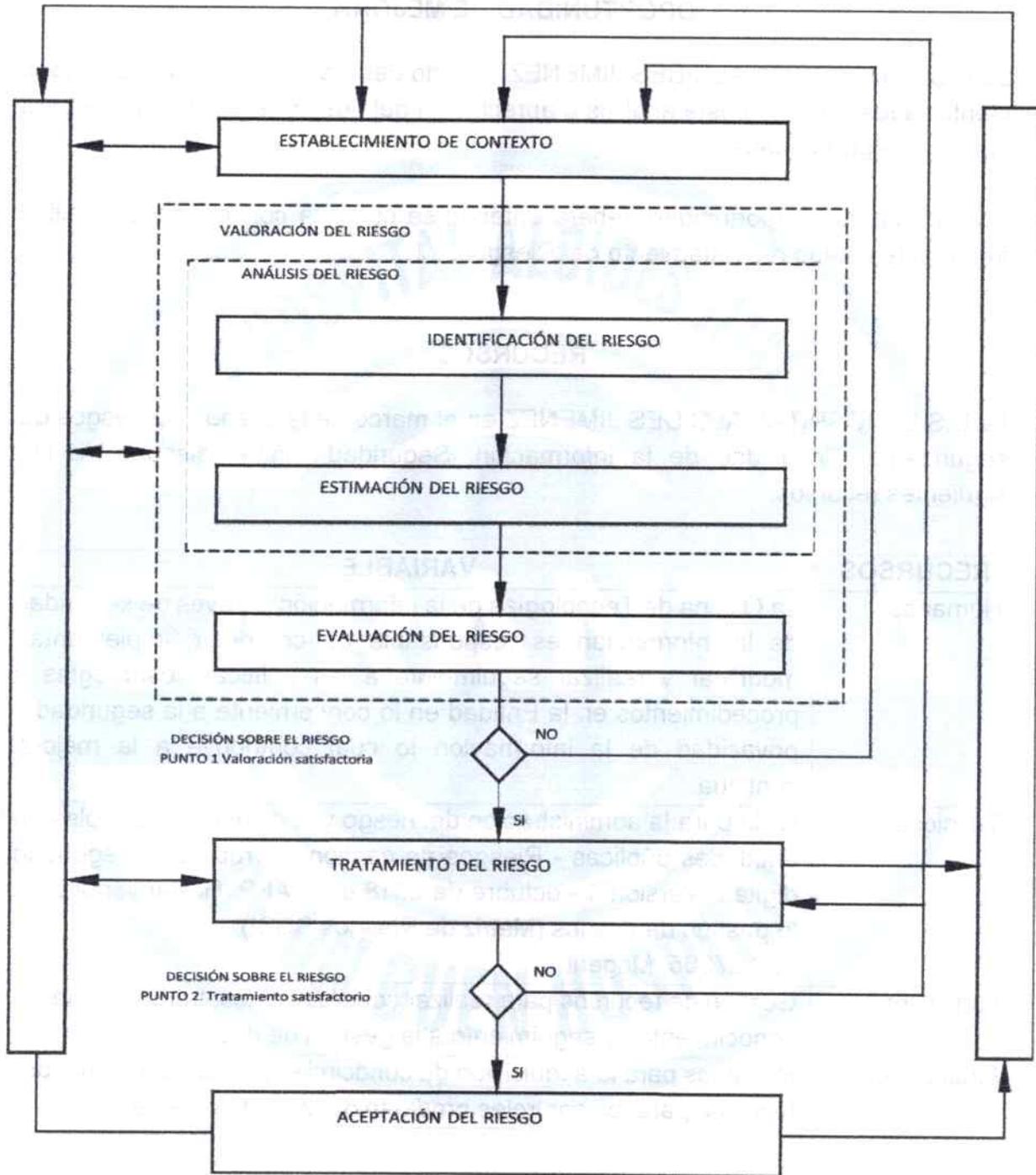


Ilustración 3. Fases Riesgos ISO 31000

ELABORADO POR: RUBÉN DARÍO GUZMÁN VALLEJO	REVISADO POR: BYRON STEVEN AGUDELO	APROBADO POR: ESTEBAN LÓPEZ BURBANO
CARGO: ING. DE SISTEMAS	CARGO: Subgerente	CARGO: Gerente
FECHA: 17 de Enero de 2025	FECHA: 17 de Enero de 2025	FECHA: 17 de Enero de 2025

	E.S.E HOSPITAL ALCIDES JIMENEZ NIT. 846.001.669-0	VERSIÓN: 02	CÓDIGO: AD-PL- 002
	PLAN DE TRATAMIENTO DE RIESGO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2025	FECHA DE ACTUALIZACIÓN 17 de Enero de 2025	
		PAGINA: 14 DE 15	

OPORTUNIDAD DE MEJORA

La E.S.E. HOSPITAL ALCIDES JIMENEZ no sólo deberá centrarse en los riesgos identificados, sino que este análisis o apreciación del riesgo debe ser la base para identificar oportunidades.

Por lo anterior la oportunidad deberá entenderse como la consecuencia positiva frente al resultado del tratamiento del Riesgo.

RECURSOS

La E.S.E. HOSPITAL ALCIDES JIMENEZ en el marco de la gestión de riesgos de seguridad y Privacidad de la información, Seguridad Digital, dispone de los siguientes recursos.

RECURSOS	VARIABLE
Humanos	La Oficina de Tecnologías de la información a través de seguridad de la información es responsable de coordinar, implementar, modificar y realizar seguimiento a las políticas, estrategias y procedimientos en la Entidad en lo concerniente a la seguridad y privacidad de la información lo cual contribuye a la mejora continua.
Técnicos	Guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital - Versión 4 - octubre de 2018 del DAFP. Herramienta para la gestión de riesgos (Matriz de Riesgos SGSI), ISO 27005, Magerit
Logísticos	Gestión de recursos para realizar socializaciones, transferencia de conocimientos y seguimiento a la gestión de riesgos.
Financieros	Recursos para la adquisición de conocimiento, recursos humanos, técnicos para los controles producto de la gestión de riesgos

ELABORADO POR: RUBÉN DARÍO GUZMÁN VALLEJO	REVISADO POR: BYRON STEVEN AGUDELO	APROBADO POR: ESTEBAN LÓPEZ BURBANO
CARGO: ING. DE SISTEMAS	CARGO: Subgerente	CARGO: Gerente
FECHA: 17 de Enero de 2025	FECHA: 17 de Enero de 2025	FECHA: 17 de Enero de 2025

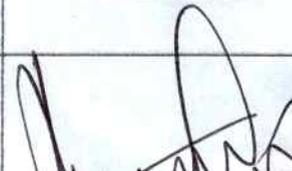
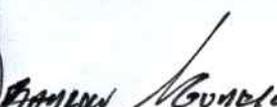
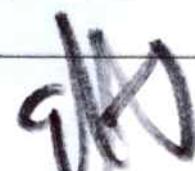
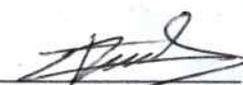
"Documento controlado del Sistema de Gestión de Calidad de la E.S.E Hospital Alcides Jiménez. Su Reproducción no es válida sin autorización".

 E.S.E HOSPITAL ALCIDES JIMENEZ NIT. 846.001.669-0	VERSIÓN: 02	CÓDIGO: AD-PL-002
	PLAN DE TRATAMIENTO DE RIESGO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2025	
	FECHA DE ACTUALIZACIÓN 17 de Enero de 2025	
	PAGINA: 15 DE 15	

PRESUPUESTO

La estimación y asignación del presupuesto para el plan de tratamiento de riesgos de Seguridad y Privacidad de la información identificados en la entidad, corresponderá al dueño del riesgo, quien es el responsable de contribuir con el seguimiento y control de la gestión, además de la implementación de los controles definidos en el plan de tratamiento, como la gestión de sus recursos dentro de la planificación de los mismos.

APROBACIÓN

	Elaborado por:	Revisado por:	Revisado por:	Aprobado por:
Nombre	 RUBÉN DARÍO GUZMÁN VALLEJO	 ANGY MAGALY GILÓN TORO	 BYRON STIVEN AGUDELO	 ESTEBAN LÓPEZ BURBANO
Cargo	Ing. de sistemas	Auditora de Calidad	Subgerente	Gerente
Nombre	 DIEGO ARMANDO ERASO			
Cargo	Técnico de sistemas			

ELABORADO POR: RUBÉN DARÍO GUZMÁN VALLEJO	REVISADO POR: BYRON STEVEN AGUDELO	APROBADO POR: ESTEBAN LÓPEZ BURBANO
CARGO: ING. DE SISTEMAS	CARGO: Subgerente	CARGO: Gerente
FECHA: 17 de Enero de 2025	FECHA: 17 de Enero de 2025	FECHA: 17 de Enero de 2025

"Documento controlado del Sistema de Gestión de Calidad de la E.S.E Hospital Alcides Jiménez. Su Reproducción no es válida sin autorización".