RESOLUCION Nº 13-430-16-42-00-028 DE 2026.
(enero 26)

"POR MEDIO DEL CUAL SE ADOPTA EL PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN EN LA ESE HOSPITAL LA DIVINA MISERICORDIA PARA LA VIGENCIA 2026".
RESUELVE:

ARTÍCULO 1°: ADOPTAR. Adoptar el Plan de tratamiento de riesgos de seguridad y privacidad de la información en la Empresa Social del Estado Hospital La Divina Misericordia para la vigencia 2026, el cual se encuentra anexo y hace parte integral del presente acto administrativo, contenido en veinticinco (25) folios.

ARTÍCULO 2°. ÁMBITO DE APLICACIÓN. El Plan de tratamiento de riesgos de seguridad y privacidad de la información será asumido y cumplido de manera consiente y responsable por todos los servidores públicos de la Empresa Social del Estado Hospital La Divina Misericordia en todos los niveles y jerarquías, sin perjuicio de las normas, códigos o manuales vigentes y tendrán la obligación de cooperar en la ejecución de las actividades programadas en ello.

ARTÍCULO 3°. ACTUALIZACIONES. Realizar las actualizaciones correspondientes cuando la estructura del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información para la vigencia 2026 asi lo requiera.

ARTÍCULO 4º. SEGUIMIENTO. El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la información para la vigencia 2026 será objeto de seguimiento por parte del Jefe de Control Interno o quien hagas sus veces.

ARTÍCULO 4º. PUBLICACIÓN Y DIVULGACIÓN. Las actividades incluidas en el plan adoptado en la presente resolución, deberán ser divulgadas por medio de los canales de comunicación que se dispongan en la Empresa Social del Estado Hospital La Divina Misericordia, en especial deberá ser publicado en el link de transparencia dispuesto en su página web.

ARTÍCULO 5º. La presente resolución rige a partir de la fecha de su expedición.

PUBLIQUESE, COMUNÍQUESE Y CÚMPLASE

Dado en Magangué, Bolívar a los veintiséis (26) días del mes de enero del 2026.

CANDELARIA VALDELAMAR MARTINEZ
Gerente de la E.S.E. Hospital La Divina Misericordia

	Nombre	Cargo	Firma
Proyectó	Omar Cuello Posada	Asesor del Area de Talento Humano ESE HLDM	
Revisó	Elsi Sampayo Benavides	Asesora Jurídica ESE HLDM	
Los arriba firmantes declaramos que hemos revisado el presente documento y lo encontramos ajustado a las normas y disposiciones legales vigentes y por lo tanto, bajo nuestra responsabilidad lo presentamos para la firma.			

RESOLUCION Nº 13-430-16-42-00-028 DE 2026.
(enero 26)

"POR MEDIO DEL CUAL SE ADOPTA EL PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN EN LA ESE HOSPITAL LA DIVINA MISERICORDIA PARA LA VIGENCIA 2026".

La Representante Legal de la **EMPRESA SOCIAL DEL ESTADO HOSPITAL LA DIVINA MISERICORDIA**, en uso de sus facultades constitucionales, legales y en especial las conferidas en la Ley 100 del 1993, Decreto 1876 de 1994, Decreto 612 del 2018 y

CONSIDERANDO:

1. Que mediante Decreto 415 de 2016, se adicionó al Decreto 1083 de 2015, todo lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las telecomunicaciones.

2. Que el Decreto 1078 de 2018, contempla en el artículo 2.2.9.1.2.2. los instrumentos para implementar la estrategia de Gobierno en Linea, dentro de los cuales se exige la elaboración por parte de cada entidad de un Plan de Seguridad y Privacidad de la Información.

3. Que mediante el Decreto 1008 de 2018 se establece que la Seguridad y la Privacidad de la Información es uno de los habilitadores transversales de la Nueva Política de Gobierno Digital.

4. Que mediante el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, se busca proteger la integridad, garantizar la disponibilidad y confidencialidad de todos los activos de información de la entidad.

5. Que el Decreto 612 de 2018 en su artículo 1 adiciona el capítulo 3 del título 22 de la parte 2 de libro 2 del Decreto 1083 de 2015 Único Reglamentario del Sector de Función Pública, en el siguiente artículo: 2.2.22.3.14. Integración de los planes institucionales y estratégicos al Plan de Acción. "*Las entidades del Estado, de acuerdo con el ámbito de aplicación del Modelo Integrado de Planeación y Gestión, al Plan de Acción de que trata el artículo 74 de la Ley 1474 de 2011, deberán integrar los planes institucionales y estratégicos que se relacionan a continuación y publicarlo en su respectiva página web, a más tardar el 31 de enero de cada año*", dentro de los cuales se encuentra el Plan de tratamiento de riesgos de seguridad y privacidad de la información.

6. Que para dar cumplimiento a las disposiciones legales mencionadas anteriormente y atendiendo a las necesidades en la Empresa Social del Estado Hospital La Divina Misericordia, se adoptó el Plan de tratamiento de riesgos de seguridad y privacidad de la información para la vigencia 2026.

7. Que de conformidad con lo expuesto,

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

VIGENCIA 2026

INTRODUCCIÓN

Si en un principio los factores de riesgo estaban asociados principalmente a contingencias de carácter natural y tecnológico, las consecuencias derivadas de sucesos posteriores y relevantes como el terrorismo, la inestabilidad política, las pandemias y los códigos maliciosos, entre otros, han señalado la necesidad de incorporar nuevas amenazas presentes no solamente en el mundo físico sino también en el entorno digital, cuando se trate de comprender los riesgos más significativos a los activos de información.

El análisis de riesgos de los activos de información permite entender de una manera efectiva y eficiente, los riesgos de pérdida de confidencialidad, integridad y disponibilidad sobre cada uno de los activos definidos como parte del alcance del análisis. Gestionar eficazmente la seguridad de la información y riesgos de seguridad digital de los sistemas de información de la entidad, así como en los activos que participan en sus procesos y que se encuentran expuestos, permite garantizar la confidencialidad, integridad y disponibilidad de la información a través de la aplicación de las opciones apropiadas de tratamiento de riesgos de Seguridad de la información y seguridad digital, teniendo en cuenta la evaluación de los resultados de la valoración de los riesgos del Sistema de Gestión de Seguridad de la Información y en concordancia a la normativa aplicable.

El plan de tratamiento de riesgos de seguridad apoya la implementación de controles y acciones tendientes a la mitigación de los riesgos del proceso de gestión tecnológica, hallazgos de auditorías internas y apoya el cumplimiento del Modelo integrado de planeación y gestión dentro de su política de gobierno Digital.

Dirección: Barrió San José ave. Colombia N° 13 -146- Tel: 6888223
misericordia@esehospitalladivinamisericordia.gov.co

TABLA DE CONTENIDO

Dirección: Barrió San José ave. Colombia N° 13 -146- Tel: 6888223
misericordia@esehospitalladivinamisericordia.gov.co

1. OBJETIVOS

1.1. OBJETIVO GENERAL

Presentar el Plan de Tratamiento para los riesgos de seguridad y privacidad de la información, identificados en los procesos incluidos en el alcance del SGSI de la Empresa Social del Estado Hospital La Divina Misericordia para la vigencia 2026.

1.2. OBJETIVOS ESPECÍFICOS

- Definir y aplicar los lineamientos para tratar de manera integral los riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación que la ESE pueda estar expuesto y de esta manera alcanzar los objetivos, la misión y la visión institucional, protegiendo y preservando la integridad, confidencialidad, disponibilidad y autenticidad de la información.
- Cumplir con los requisitos legales y reglamentarios pertinentes a la legislación colombiana.
- Gestionar riesgos de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la operación, de acuerdo con los contextos establecidos en la entidad.
- Fortalecer y apropiar conocimiento referente a la gestión de riesgos seguridad y privacidad de la información, seguridad digital y continuidad de la operación.

2. NORMATIVIDAD

- Decreto 1078 de 2015: Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- Decreto 1008 de 2018: Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.
- CONPES 3854 de 2016: Política Nacional de Seguridad Digital

Dirección: Barrió San José ave. Colombia N° 13 -146- Tel: 6888223
misericordia@esehospitalladivinamisericordia.gov.co

- Manual para la Implementación de la Política de Gobierno Digital: Implementación de la política de Gobierno Digital. Decreto 1008 de 2018 (Compilado en el Decreto 1078 de 2015, capítulo 1, título 9, parte 2, libro 2) Versión 7, abril de 2019.
- Modelo de Seguridad y privacidad de la información – MSPI: Se encuentra alineado con el Marco de Referencia de Arquitectura TI y soporta transversalmente los otros componentes de la Política de Gobierno Digital, TIC para el Estado y TIC para la Sociedad. TIC, que son habilitados por tres elementos transversales: Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales.
- NTC / ISO 27001:2013: Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI).
- NTC/ISO 31000:2009: Gestión del Riesgo. Principios y directrices
- Guía para la administración del riesgo y el diseño de controles en entidades públicas–Versión 5: Riesgos de Gestión, Corrupción y Seguridad Digital Función Pública. 2020.

3. DEFINICIONES

- Activo: cualquier elemento que tenga valor para la organización.
- Análisis del riesgo: Se estima el riesgo con el fin de proporcionar bases que logre la evaluación y la naturaleza del riesgo.
- Causa: Elemento específico que origina el evento.
- Contexto externo: Ambiente externo en el cual la organización busca alcanzar sus objetivos (tecnológico, legal, regional, etc.).
- Contexto interno: Ambiente interno en el cual la organización busca alcanzar sus objetivos (gobierno, políticas, estructura organizacional, etc.).
- Controles: Procesos, políticas y/o actividades que pueden modificar el riesgo.
- Criterios de riesgos: Términos de referencia frente a los cuales se evaluará la importancia del riesgo.
- Evaluación del Riesgo: Comparar los resultados del análisis de riesgo frente a los controles implementados, con el fin de determinar el riesgo final.
- Evento: Posible ocurrencia de Incidente o amenaza de Seguridad de la Información.

Dirección: Barrió San José ave. Colombia N° 13 -146- Tel: 6888223
misericordia@esehospitalladivinamisericordia.gov.co

- Fuente: Elemento que por sí solo o en combinación tiene el potencial intrínseco para dar lugar a riesgo; a fuente del riesgo puede ser tangible o intangible.
- Gestión del riesgo: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.
- Identificación del riesgo: Se determinan las causas, fuentes del riesgo y los eventos con base al contexto el proceso, que pueden afectar el logro de los objetivos del mismo.
- Riesgo aceptable: Riesgo en que la organización decide que puede convivir y/o soportar dado a sus obligaciones legales, contractuales y/o intereses propios.
- Riesgo residual: Nivel de riesgo que permanece luego de tomar medidas de tratamiento.
- Riesgo: Posibilidad o probabilidad de que un evento pueda afectar las funciones de la entidad e impactar el logro de sus objetivos.
- Riesgo de seguridad digital: combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas.

4. ALCANCE

Realizar una eficiente gestión de riesgos de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación, que permita integrar en los procesos de la entidad, buenas prácticas que contribuyan a la toma de decisiones y prevenir incidentes que puedan afectar el logro de los objetivos. Junto con Guía de Gestión de Riesgos de Seguridad y Privacidad de la Información (MinTIC: 2016): se dan los lineamientos para poder identificar, analizar, tratar, evaluar y monitorear los riesgos de seguridad y privacidad de la información en la Empresa Social del Estado Hospital La Divina Misericordia.

El Plan de Tratamiento de Riesgo tendrá en cuenta los riesgos que se encuentren en los niveles Alto y Extremo acorde con los lineamientos definidos por el Ministerio TIC, los riesgos que se encuentren en niveles inferiores serán manejados por la entidad, a fin de evitar la materialización de los mismos.

Dirección: Barrió San José ave. Colombia N° 13 -146- Tel: 6888223
misericordia@esehospitalladivinamisericordia.gov.co

5. MARCO REFERENCIAL

La Empresa Social del Estado Hospital La Divina Misericordia a través de su Modelo Integrado de Gestión, se compromete a mantener una cultura de la gestión del riesgo asociados con la responsabilidad de diseñar, adoptar y promover las políticas, planes, programas y proyectos del sector TIC, regulando los riesgos de 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 de la Empresa Social del Estado Hospital La Divina Misericordia.

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 (MinTIC:2016)1 , 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"(...).

6. PRINCIPIOS DE LA GESTIÓN DE RIESGOS

Integrada	La gestión del riesgo es parte integral de todas las actividades de la organización.
Estructurada y exhaustiva	Un enfoque estructurado y exhaustivo hacia la

Dirección: Barrió San José ave. Colombia N° 13 -146- Tel: 6888223
misericordia@esehospitalladivinamisericordia.gov.co

	gestión del riesgo contribuye a resultados coherentes y comparables.
Adaptada	El marco de referencia y el proceso de la gestión del riesgo se adaptan y son proporcionales a los contextos externo e interno de la organización relacionados con sus objetivos.
Inclusiva	La participación apropiada y oportuna de las partes interesadas permite que se consideren su conocimiento, puntos de vista y percepciones.
Dinámica	Los riesgos pueden aparecer, cambiar o desaparecer con los cambios de los contextos externo e interno de la organización. La gestión del riesgo anticipa, detecta, reconoce y responde a esos cambios y eventos de una manera apropiada y oportuna.
Mejor Información Disponible	Las entradas a la gestión del riesgo se basan en información histórica y actualizada, así como en expectativas futuras.
Factor humano	El comportamiento humano y la cultura influyen considerablemente en todos los aspectos de la gestión del riesgo en todos los niveles y etapas.
Mejora continua	La gestión del riesgo mejora continuamente mediante el aprendizaje y experiencia.

Dirección: Barrió San José ave. Colombia N° 13 -146- Tel: 6888223
misericordia@esehospitalladivinamisericordia.gov.co

7. OBJETIVOS DEL ANÁLISIS Y GESTIÓN DE LOS RIESGOS

Crear valor y proteger	Contribuye a la consecución de los objetivos demostrables y la mejora del rendimiento.
Ser parte integral de los procesos	Forma parte de las responsabilidades de gestión y de los procesos.
Apoyo para la toma de decisiones	Ayuda a tomar decisiones y priorizar acciones.
Contemplar la explícitamente incertidumbre.	Contemplar la explícitamente incertidumbre.
Aportar a la mejora continua de la organización.	Mejorar su grado de madurez de gestión de riesgos.

8. MARCO DE REFERENCIA

8.1. ROLES Y RESPONSABILIDADES

La gestión del riesgo se desarrolla bajo el esquema de líneas de defensa, modelo de control que establece y clasifica los roles y responsabilidades de todos los actores del riesgo, para proporcionar aseguramiento de la gestión y prevenir la materialización de los riesgos. Los roles establecidos son:

- Línea Estratégica
- Primera Línea de Defensa
- Segunda Línea de Defensa
- Tercera Línea de Defensa.

Línea de defensa	Rol	Responsabilidad
Línea Estratégica	Alta Gerencia (Gerente).	Revisar los cambios en el direccionamiento estratégico del contexto y dar las directrices para evaluar la necesidad de actualizar

Dirección: Barrió San José ave. Colombia N° 13 -146- Tel: 6888223
misericordia@esehospitalladivinamisericordia.gov.co

		los documentos de riesgos de la entidad.
		Solicitar a los responsables de los procesos la revisión de los riesgos y el seguimiento de las acciones de control.
		Revisar los informes emitidos por las unidades de gestión encargadas de la evaluación y control, sobre los resultados de las acciones para el tratamiento de riesgos
		Hacer seguimiento a las acciones de tratamiento de los riesgos para garantizar el cumplimiento de las líneas y que los procesos tomen acciones de mejora continua.
Primera linea	Responsable del proceso de tecnología de la información	Apropiar documentos al interior del proceso con el fin de determinar actividades de control.
		Analizar los riesgos identificados determinando la probabilidad de ocurrencia y consecuencias para establecer el riesgo inherente.
		Diseñar y clasificar controles para el tratamiento de riesgos.

Dirección: Barrió San José ave. Colombia N° 13 -146- Tel: 6888223
misericordia@esehospitalladivinamisericordia.gov.co

		Aplicar en las frecuencias establecidas los controles definidos dejando la documentación correspondiente.
		Tratar los riesgos definidos mediante implementación de actividades con el fin de reducir su materialización.
		Definir acciones de contingencia y aplicarlas en caso de materialización de los riesgos.
		Coordinar con el recurso humano el seguimiento y la apropiación de las acciones de control.

Dirección: Barrió San José ave. Colombia N° 13 -146- Tel: 6888223
misericordia@esehospitalladivinamisericordia.gov.co

Segunda línea	Supervisores contractuales	Hacer seguimiento, evaluación y monitoreo de los riesgos definidos en los procesos durante la ejecución de los contratos hasta la liquidación.
	Responsables de acompañamiento de calidad.	Apoyar la actualización los documentos y herramientas de gestión conforme a los avances de tratamiento del riesgo.
Tercera línea	Oficina de control interno o quien cumpla estas funciones.	Realizar el seguimiento periódico al tratamiento de riesgos y a las actividades definidas en el mismo, con el fin de generar acciones que evidencien los avances en el tratamiento del riesgo y la mejora continua.
		Evaluar de manera objetiva la efectividad del tratamiento y la gestión realizada a los riesgos identificados por la entidad.

Dirección: Barrió San José ave. Colombia N° 13 -146- Tel: 6888223
misericordia@esehospitalladivinamisericordia.gov.co

		Llevar a cabo el seguimiento a los riesgos y la actualización en los documentos de gestión referente al avance en el tratamiento de los mismos.
		Revisar la aplicación de los controles e instrumentos de gestión relacionados al tratamiento y la gestión de riesgos.

8.2. INSTITUCIONALIDAD

Conforme a lo establecido en la guía de administración del riesgo del DAFP, el modelo integrado de planeación y gestión (MIPG) define para su operación articulada la creación en todas las entidades del Comité Institucional de Gestión y Desempeño, regulado por el Decreto 1499 de 2017 y el Comité Institucional de Coordinación de Control Interno, reglamentado a través del artículo 13 de la Ley 87 de 1993 y el Decreto 648 de 2017, en este marco general, para una adecuada gestión del riesgo.

8.3. BENEFICIOS

Considerando que la gestión del riesgo es un proceso efectuado por la alta dirección de la entidad y por todo el personal con el propósito de proporcionar a la entidad un aseguramiento razonable con respecto al logro de los objetivos, los principales beneficios para la entidad son los siguientes:

- Apoyo a la toma de decisiones.

Dirección: Barrió San José ave. Colombia N° 13 -146- Tel: 6888223
misericordia@esehospitalladivinamisericordia.gov.co

- Garantizar la operación normal de la organización.
- Minimizar la probabilidad e impacto de los riesgos.
- Mejoramiento en la calidad de procesos y sus servidores (calidad va de la mano con riesgos).
- Fortalecimiento de la cultura de control de la organización.
- Incrementa la capacidad de la entidad para alcanzar sus objetivos.
- Dota a la entidad de herramientas y controles para hacer una administración más eficaz y eficiente.

9. CRONOGRAMA

El Plan de Tratamiento de Riesgos de seguridad y privacidad de la información contempla la definición de las actividades a desarrollar en aras de mitigar los riesgos sobre los activos.

Dirección: Barrió San José ave. Colombia N° 13 -146- Tel: 6888223
misericordia@esehospitalladivinamisericordia.gov.co

GESTION	ACTIVIDAD	TAREA	RESPONSABLE
GESTION DE RIESGOS	Actualización de lineamientos de riesgos	Actualizar política y metodología de gestión de riesgos	Gerencia o su delegado
	Sensibilización	Socialización guía y herramientas- Gestión de riesgos de seguridad y privacidad de la información, seguridad digital y continuidad de la operación.	Gerencia o su delegado
	Identificación de riesgos de seguridad y privacidad de la información, seguridad digital y continuidad de la operación	Identificación, análisis y evaluación de los riesgos de seguridad y privacidad de la información, seguridad digital y continuidad de la operación.	Lideres de procesos.
		.Retroalimentación, revisión y verificación de los riesgos identificados (ajustes).	Gerencia o su delegado
	Aceptación de riesgos identificados	Aceptación, aprobación de riesgos identificados y planes de mejoramiento.	Lideres de procesos.
	Publicación	Publicación de la matriz de riesgos.	Gerencia o su delegado
	Seguimiento fase de tratamiento	Seguimiento estado de planes de tratamiento de riesgos identificados y verificación de evidencia.	Control Interno
	Evaluación de riesgos residuales	Evaluación de riesgos residuales.	Lideres de procesos.
	Mejoramiento	Identificación de oportunidades de mejora acorde a los resultados obtenidos durante las evaluaciones de riesgos residuales.	Lideres de procesos.
		Actualización de riesgos de seguridad de acuerdo a los cambios solicitados.	Lideres de procesos.
	Monitoreo y revisión.	Generación, presentación y reporte de indicadores	Control Interno

Dirección: Barrió San José ave. Colombia N° 13 -146- Tel: 6888223
misericordia@esehospitalladivinamisericordia.gov.co

9.1. DESARROLLO METODOLÓGICO

La gestión del riesgo dentro de la seguridad de la información se enmarca dentro del ciclo de planear, hacer, verificar y actuar (PHVA) tal como se muestra en la siguiente ilustración (ISO 27001:2013):

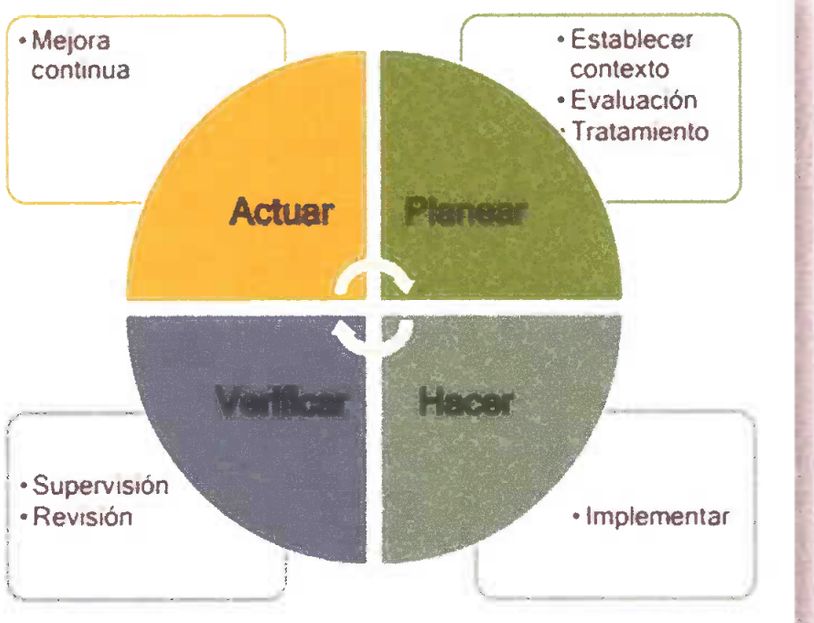


Ilustración 2. Ciclo PHVA y la gestión de riesgos

La técnica de análisis de riesgo para activos de información permite desde un punto de vista orientado a la empresa y sistémico en su naturaleza, comprender claramente los riesgos sobre los activos de información a los que puede estar expuesto la Empresa Social del Estado Hospital La Divina Misericordia.

Dirección: Barrió San José ave. Colombia N° 13 -146- Tel: 6888223
misericordia@esehospitalladivinamisericordia.gov.co

Es recomendable contar con técnicas para identificar los riesgos específicos asociados a los activos y complementar este proceso en la medida de lo posible con la identificación de puntos críticos de fallas, análisis de disponibilidad, análisis de vulnerabilidad, análisis de confiabilidad y árboles de falla. El plan propuesto en este documento comprende, como se detallará más adelante, las siguientes actividades principales: establecimiento del contexto, identificación riesgos, estimación de riesgos, evaluación de riesgos, tratamiento de riesgo y aceptación del riesgo, guardando coherencia con la Guía para la administración del riesgo y el diseño de controles en entidades públicas V5, emitida por el Departamento Administrativo de la Función Pública.

Ilustración 1. Estructura general de la metodología de riesgos

El proceso de identificación y evaluación de los riesgos de seguridad de la información está compuesto por los siguientes Hitos o actividades:

Dirección: Barrió San José ave. Colombia N° 13 -146- Tel: 6888223
misericordia@esehospitalladivinamisericordia.gov.co

- Programación y agendamiento de entrevistas. En esta fase se seleccionan los procesos incluidos en el alcance del SGSI de la ESE y se procede a programar y a agendar a los líderes de las dependencias y grupos internos de trabajo que conforman los procesos, para la identificación de riesgos.
- Entrevista con los Líderes. Se entrevista a cada líder de dependencia o grupo, se presenta la metodología y en conjunto se procede a realizar la identificación de los riesgos sobre los activos de información, los cuales se consignan en la Matriz de Riesgos.
- Identificación y Calificación de Riesgos. En esta fase, el líder de proceso evalúa el nivel de impacto vs. Probabilidad y los controles existentes para calcular el nivel de riesgo.

A continuación se dan a conocer los criterios que tiene establecido Empresa Social del Estado Hospital La Divina Misericordia para calificar la probabilidad e impacto de los riesgos de seguridad y privacidad de la información.

CRITERIOS PARA CALIFICAR LA PROBABILIDAD RIESGOS SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

NIVEL	DESCRIPTOR	CRITERIOS DE FACTIBILIDAD	CRITERIOS DE FRECUENCIA
5	CASI SEGURO	Se espera que el evento suceda en la mayoría de circunstancias.	Más de 1 vez al año.
4	PROBABLE	Es viable que el evento suceda en la mayoría de circunstancias.	Al menos 1 vez en el último año.
3	POSIBLE	El evento podrá ocurrir en cualquier evento	Al menos 1 vez en los 2 últimos años.
2	IMPROBABLE	El evento puede ocurrir	Al menos 1 vez en los

Dirección: Barrió San José ave. Colombia N° 13 -146- Tel: 6888223
misericordia@esehospitalladivinamisericordia.gov.co

		en algún momento.	últimos 5 años.
1	RARA VEZ	El evento puede ocurrir en circunstancias excepcionales.	No se ha presentado en los últimos 5 años.

Fuente: Adaptado de la Guía para la administración del riesgo y el diseño de controles en entidades públicas versión 4 emitida en Octubre del 2018.

En caso de que la entidad no cuente con datos históricos sobre el número de eventos que se hayan materializado en un periodo de tiempo, los integrantes del equipo de trabajo deben calificar en privado el nivel de probabilidad en términos de factibilidad.

CRITERIOS DE IMPACTO PARA LOS RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

NIVEL	VALOR DEL IMPACTO	IMPACTO CONSECUENCIAS(CUALITATIVO)
CATASTRÓFICO	5	Afectación muy grave de la integridad de la información debido al interés particular de los empleados y terceros. Afectación muy grave de la disponibilidad de la información debido al interés particular de los empleados y terceros. Afectación muy grave de la confidencialidad de la información debido al interés particular de los empleados y terceros.
MAYOR	4	Afectación grave de la integridad de la información debido al interés particular de los empleados y terceros. Afectación grave de la disponibilidad de la información debido al interés particular de los empleados y terceros. Afectación grave de la confidencialidad de la información debido al interés particular de los empleados y terceros.
MODERADO	3	Afectación moderada de la integridad de la información debido al interés particular de los empleados y terceros. Afectación moderada de la

Dirección: Barrió San José ave. Colombia N° 13 -146- Tel: 6888223
misericordia@esehospitalladivinamisericordia.gov.co

		disponibilidad de la información debido al interés particular de los empleados y terceros. Afectación moderada de la confidencialidad de la información debido al interés particular de los empleados y terceros.
MENOR	2	Afectación leve de la integridad. Afectación leve de la disponibilidad. Afectación leve de la confidencialidad.
INSIGNIFICANTE	1	Sin afectación de la integridad. Sin afectación de la disponibilidad. Sin afectación de la confidencialidad.

Fuente: Adoptado del Ministerio de Tecnologías de la Información y las Comunicaciones. 2017. Criterios De Impacto Para Riesgos De Seguridad Digital.

- Valoración del Riesgo Residual. En esta fase se hace una proyección de la eficacia de los controles para calcular el riesgo residual.

- Mapas de calor donde se ubican los riesgos. Luego se procede a ubicar los riesgos en un mapa de calor para visualizar su comportamiento a medida que se van aplicando los controles.

9.1.1. TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACION

Una vez ejecutadas las etapas de análisis y valoración de riesgos y con base en los resultados obtenidos en la determinación real de riesgos, es necesario tomar decisiones aplicando el apetito de riesgos definido por la Empresa Social del Estado Hospital La Divina Misericordia.

Para el manejo de los riesgos serán tomados en cuenta lo establecido en la Guía para la administración del riesgo y el diseño de controles en entidades públicas versión 5 emitida en Diciembre del 2020 expedida por el Departamento Administrativo de la Función pública, pág. 57.

Dirección: Barrió San José ave. Colombia N° 13 -146- Tel: 6888223
misericordia@esehospitalladivinamisericordia.gov.co

El Departamento Administrativo de la Función pública manifiesta que el tratamiento de los riesgos es la respuesta establecida por la primera línea de defensa para la mitigación de los diferentes riesgos. De allí, que la respuesta dada al riesgo se enmarca en las siguientes categorías:

- ✓ **REDUCIR EL RIESGO:** Después de realizar un análisis y considerar que el nivel de riesgo es alto, se determina tratarlo mediante transferencia o mitigación del mismo.
- ✓ **MITIGAR EL RIESGO:** Después de realizar un análisis y considerar los niveles de riesgos se implementan acciones que mitiguen el nivel de riesgo. No necesariamente es un control adicional.
- ✓ **TRANSFERIR EL RIESGO:** Después de realizar un análisis, se considera que la mejor estrategia es tercerizar el proceso o trasladar el riesgo a través de seguros o pólizas. La responsabilidad económica recae sobre el tercero, pero no se transfiere la responsabilidad sobre el tema reputacional.
- ✓ **ACEPTAR EL RIESGO:** Después de realizar un análisis y considerar los niveles de riesgo se determina asumir el mismo, conociendo los efectos de su posible materialización. (Ningún riesgo de corrupción podrá ser aceptado).
- ✓ **EVITAR EL RIESGO:** Después de realizar un análisis y considerar que el nivel de riesgo es demasiado alto, se determina NO asumir la actividad que genera este riesgo.

Fuente: Adaptado de la Guía para la administración del riesgo y el diseño de controles en entidades públicas versión 5 emitida en Diciembre del 2020.

NIVELES DE ACEPTACIÓN AL RIESGO

A partir de los criterios Reducir, Mitigar, Transferir, Aceptar y Evitar, en la Empresa Social del Estado Hospital La Divina Misericordia, se establecen los siguientes niveles de aceptación y periodicidad de seguimiento de los riesgos identificados:

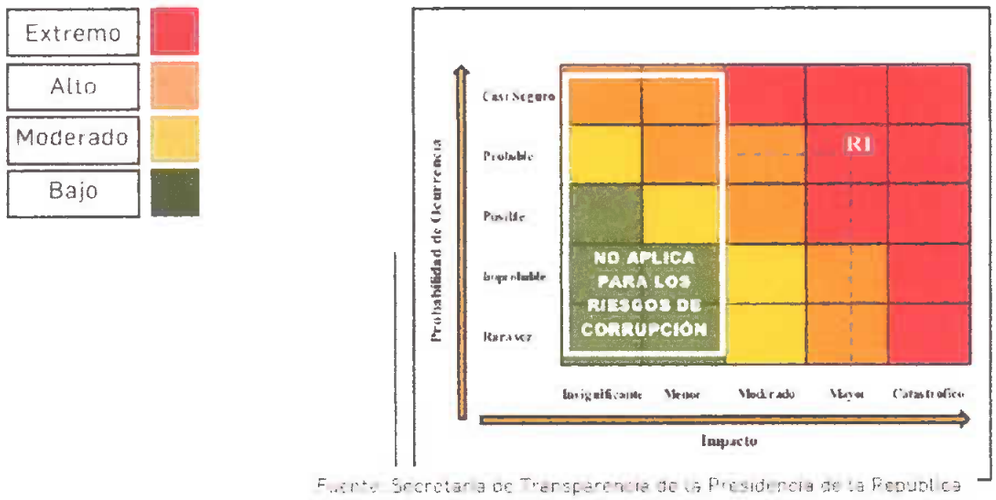
Zona de riesgo baja: Aceptar o Mitigar el riesgo. Nota: Los riesgos de corrupción son inaceptables. Se administra por medio de actividades propias del proceso asociado.

Dirección: Barrió San José ave. Colombia N° 13 -146- Tel: 6888223
misericordia@esehospitalladivinamisericordia.gov.co

Zona de riesgo moderada: Mitigar el riesgo. Se establecen acciones que permitan reducir la probabilidad de ocurrencia del riesgo.

Zona de riesgo Alta: Reducir, Mitigar o Transferir. Su monitoreo debe ser permanente por cada líder de proceso.

Zona de riesgo extrema: Evitar. Se establecen acciones preventivas y correctivas que permitan evitar la materialización del riesgo. La administración de estos riesgos será con periodicidad mínima mensual. Al igual que se deben documentar al interior del proceso, planes de contingencia para tratar el riesgo materializado, con criterios de oportunidad, a fin de evitar daños en la prestación del servicio.



Fuente: Secretaría de Transparencia de la Presidencia de la República

9.2. OPORTUNIDADES DE MEJORAS

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.

10. RECURSOS

Dirección: Barrió San José ave. Colombia N° 13 -146- Tel: 6888223
misericordia@esehospitalladivinamisericordia.gov.co

La Empresa Social del Estado Hospital La Divina Misericordia en el marco de la gestión de riesgos de seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación, dispone de los siguientes recursos.

RECURSOS	VARIABLE
Humanos	La Oficina de Tecnologías de la información o quien cumpla estas funciones, a través de la 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 de Guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital - Versión 5- Diciembre 2020 del DAFP. Herramienta para la gestión de riesgos (Matriz de Riesgos SGSI).
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 y desarrollo de auditorías.

Dirección: Barrió San José ave. Colombia N° 13 -146- Tel: 6888223
misericordia@esehospitalladivinamisericordia.gov.co

11. PRESUPUESTO

Las actividades contempladas en el Plan de Tratamientos de Riesgos de seguridad y privacidad de la información de la Empresa Social del Estado Hospital La Divina Misericordia, están sujetos a disponibilidad presupuestal.

12. SEGUIMIENTO Y REVISIÓN

El objetivo del seguimiento y la revisión es asegurar la eficacia del diseño, la implementación y los resultados del tratamiento de los riesgos.

- Para el seguimiento y la revisión, asignar responsabilidades.
- El seguimiento y la revisión incluyen planificar, recopilar y analizar información, registrar resultados y proporcionar retroalimentación.
- Los resultados del seguimiento y la revisión deberían ser incluidos en todas las actividades de gestión del desempeño, la medición informará organización.

Se debe revisar periódicamente por cada responsable de los procesos al interior de las entidades, junto con su equipo los siguientes aspectos:

- Ajustes y modificaciones: después de su publicación y durante el respectivo año de vigencia, se podrán realizar los ajustes y las modificaciones necesarias orientadas a mejorar la matriz de riesgos. En este caso, deberán dejarse por escrito los ajustes, modificaciones o inclusiones realizadas.
- Monitoreo: en concordancia con la cultura del autocontrol al interior de la entidad, los líderes de los procesos junto con su equipo realizarán monitoreo y evaluación permanente a la gestión de riesgos.
- Seguimiento: el jefe de control interno o quien haga sus veces, debe adelantar seguimiento a la gestión de riesgos. En este sentido, es necesario que en sus procesos de auditoría interna analicen las causas, los riesgos y la efectividad de los controles incorporados en la matriz de riesgos.

Dirección: Barrió San José ave. Colombia N° 13 -146- Tel: 6888223
misericordia@esehospitalladivinamisericordia.gov.co

13. RECURSOS DOCUMENTALES

DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA. Guía para la administración del riesgo y diseño de controles en entidades públicas. Versión 5. Bogotá. 2020

ORGANIZACIÓN INTERNACIONAL DE ESTANDARIZACIÓN – ISO Norma Internacional ISO 31000. Ginebra, Suiza 2018

CANDELARIA VALDELAMAR MARTINEZ
Gerente

Dirección: Barrió San José ave. Colombia N° 13 -146- Tel: 6888223
misericordia@esehospitalladivinamisericordia.gov.co