E.S.E. HOSPITAL San Rafael DE ITAGÜÍ

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

DIEGO LEON MUÑOZ ZAPATA

GERENTE

2021

TABLA DE CONTENIDO

1. INTRODUCCIÓN

La E.S.E Hospital San Rafael de Itagüí en busca de la mejora continua implementa un método lógico y sistemático que permita identificar, analizar, evaluar, tratar, controlar y comunicar los riesgos asociados al manejo de la información de la entidad, para lograr que estos no afecten de una manera relevante los procesos y actividades de la entidad.

La E.S.E Hospital San Rafael de Itagüí, en su quehacer diario utiliza Las Tecnologías de la Información y la Comunicación (**TIC**), en cuanto al ingreso, procesamiento y reporte de información, para comunicarse con los diferentes actores del sistema de salud, lo cual implica que la E.S.E Hospital San Rafael de Itagüí sea vulnerable a ataques mal intencionados o mala manipulación de la información lo que acarrea problemas Estratégicos, Operativos, Financieros, y Tecnológicos, por lo cual este documento busca establecer una línea de trabajo que permita a la entidad evitar o mitigar los riesgos que lo rodean y lograr que su información este segura.

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 metodología emitida por el Departamento Administrativo de la Función Pública, en su versión vigente, además todos los servidores públicos, en cumplimiento de sus funciones, están sometidos a riesgos que pueden hacer fracasar una gestión; por lo tanto, es necesario tomar las medidas, para identificar las causas y consecuencias de la materialización de los riesgos. Se debe dar cumplimiento a la siguiente normatividad Decreto 1078 de 2015, y NTC/ISO 31000:2009.

2. DEFINICIONES

- **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)
- **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.
- **Administración de riesgos:** conjunto de etapas secuenciales que se deben desarrollar para el adecuado tratamiento de los riesgos.
- **Asumir el riesgo:** opción de manejo donde se acepta la pérdida residual probable, si el riesgo se materializa.
- **Auditoría:** Proceso sistemático, independiente y documentado para obtener evidencias de auditoria y obviamente para determinar el grado en el que se cumplen los criterios de auditoria. (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)
- **Ciberseguridad:** Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética.
- **Calificación del riesgo:** estimación de la probabilidad de ocurrencia del riesgo y el impacto que puede causar su materialización.

- **Compartir o transferir el riesgo:** opción de manejo que determina traspasar o compartir las pérdidas producto de la materialización de un riesgo con otras organizaciones mediante figuras como outsourcing, seguros, sitios alternos.

- **Consecuencia:** efectos que se pueden presentar cuando un riesgo se materializa.

- **Contexto estratégico:** son las condiciones internas y del entorno, que pueden generar eventos que originan oportunidades o afectan negativamente el cumplimiento de la misión y objetivos de una entidad.

- **Control:** acción o conjunto de acciones que minimiza la probabilidad de ocurrencia de un riesgo o el impacto producido ante su materialización. 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.

- **Control preventivo:** acción o conjunto de acciones que eliminan o mitigan las causas del riesgo; está orientado a disminuir la probabilidad de ocurrencia del riesgo.

- **Control correctivo:** acción o conjunto de acciones que eliminan o mitigan las consecuencias del riesgo; está orientado a disminuir el nivel de impacto del 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)

- **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 y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)

- **Evaluación del riesgo:** resultado del cruce cuantitativo de las calificaciones de probabilidad e impacto, para establecer la zona donde se ubicará el riesgo.

- **Evitar el riesgo:** opción de manejo que determina la formulación de acciones donde se prevenga la materialización del riesgo mediante el fortalecimiento de controles identificados.

- **Frecuencia:** ocurrencia de un evento expresado como la cantidad de veces que ha ocurrido un evento en un tiempo dado.

- **Identificación del riesgo:** etapa de la administración del riesgo donde se establece el riesgo con sus causas (asociadas a factores externos e internos de riesgo), consecuencias y se clasifica de acuerdo con los tipos de riesgo definidos

- **Impacto:** medida para estimar cuantitativa y cualitativamente el posible efecto de la materialización del riesgo.

- **Información:** Conjunto de datos procesados que constituyen un mensaje de conocimiento de determinada comunidad de personas.

- **Riesgo:** eventualidad que tendrá un impacto negativo sobre los objetivos de la entidad o del proceso.

- **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).

- **Vulnerabilidad**: Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

- **Parte interesada:** Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad

3. OBJETIVO GENERAL

Presentar el Plan de Tratamiento para los riesgos de seguridad y privacidad de la información, identificados en los procesos de la E.S.E Hospital San Rafael de Itagüí.

4. OBJETIVOS ESPECÍFICOS

- Dar lineamientos para la implementación de mejores prácticas de seguridad que permita identificar infraestructuras críticas en la E.S.E Hospital San Rafael de Itagüí.
- Identificar los riesgos asociados a los procesos.
- Promover el uso de mejores prácticas de seguridad de la información, para ser la base de aplicación del concepto de Seguridad Digital.
- Optimizar la gestión de la seguridad de la información al interior de las entidades.
- Orientar a las entidades en la adopción de la legislación relacionada con la protección de datos personales.
- Contribuir en el desarrollo del plan estratégico institucional y la elaboración del plan estratégico de tecnologías de la información y de las comunicaciones.

5. METAS

- Cumplir con el 90% Plan De Tratamiento De Riesgos De Seguridad Y Privacidad De La Información, para prevenir, mitigar o eliminar los riesgos.
- Realizar 100% de los controles de verificación adecuado relacionados con el respaldo y la restauración de la Información.

- Realizar 4 controles por medio del grupo interdisciplinario donde se tengan en cuenta todas las posibles variables de los procesos del Hospital san Rafael de Itagüí.
- Cumplir con la publicación a los usuarios de la Política de tratamiento de La información y datos personales.

6. ALCANCE

Realizar una eficiente gestión de riesgos de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación de los servicios, 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 la Guía de Gestión de Riesgos de Seguridad y Privacidad de la Información (MinTIC:2016), donde se dan los lineamientos para poder identificar, analizar, tratar, evaluar y monitorear los riesgos de seguridad y privacidad de la información.

El presente documento rige para los activos de información y los riesgos identificados en los procesos que seleccione la entidad como prioritarios y el tratamiento de los riesgos valorados como “Extremos” conforme se describe a continuación.

7. PROGRAMACIÓN DE ESTRATEGIAS Y ACTIVIDADES

6.1 ROLES Y RESPONSABILIDADES EN LA E.S.E HOSPITAL SAN RAFAEL DE ITAGÜÍ

Los responsables de la administración del riesgo dependen de la participación de los Alta Dirección, Responsables de los Procesos, Contratistas Y Control Interno.

Alta Dirección: es la responsable del fortalecimiento de los controles de administración del riesgo, aprueba las directrices para la administración del riesgo en la E.S.E Hospital San Rafael de Itagüí.

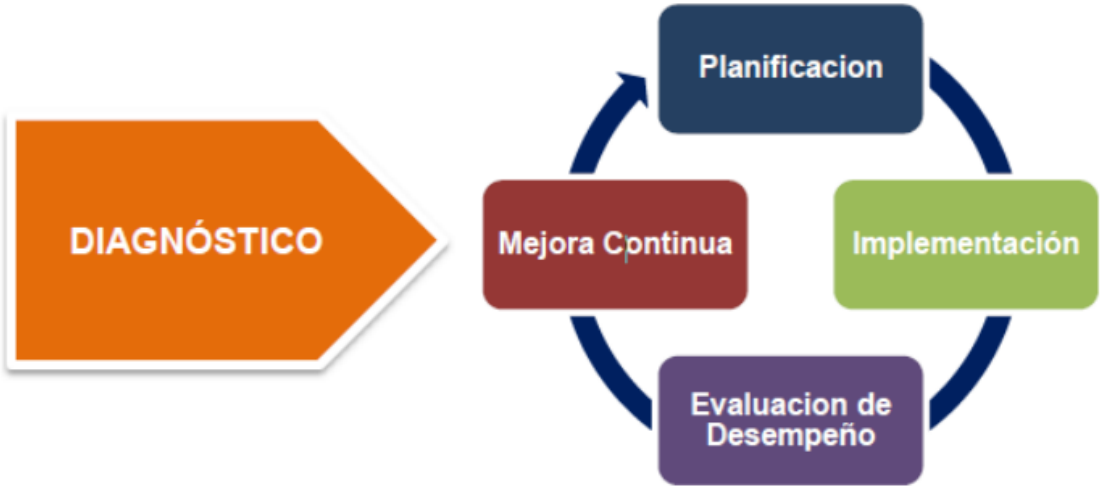
Responsables de los procesos: Es el área encargada de prevenir, mitigar y/o eliminar los riesgos, de la E.S.E Hospital San Rafael de Itagüí, al menos una vez al año. Los Líderes que apoyan la ejecución de las etapas de la administración del riesgo a nivel de los procesos, son responsable y encargados de garantizar que el proceso a su cargo, se definan los riesgos que le competen, se establezcan las estrategias y las responsabilidades para mitigarlos y que se comunique a cada funcionario de dicho proceso. No se debe olvidar que son las personas de los procesos los que mejor conocen los riesgos existentes en el desarrollo de sus actividades.

Contratistas: Debe ejecutar los controles y acciones definidas para la administración de los riesgos, aportar en la identificación de posibles riesgos que puedan afectar la Administración de los procesos en la entidad.

Control Interno: debe realizar evaluación, seguimiento y control a los procedimientos de la administración de riesgos.

6.2 DESCRIPCIÓN DEL CICLO DE OPERACIÓN

El ciclo de funcionamiento del modelo de operación, a través de la descripción detallada de cada una de las cinco (5) fases que lo comprenden, Diagnóstico, Planificación, implementación, Evolución y Mejora Continua. Estas, contienen objetivos, metas y herramientas que permiten que la seguridad y privacidad de la información sea un sistema de gestión sostenible dentro de las entidades.



Fuente: Guía del MSPI del MinTic

6.3 ETAPAS PARA LA ADMINISTRACIÓN DEL RIESGO

Las etapas para desarrollar durante la administración del riesgo de seguridad y privacidad de la información, se desplegarán los aspectos conceptuales y operativos que se deben tener en cuenta.

Identificación: El propósito de la identificación del riesgo es determinar que podría suceder que cause una perdida potencial y llegar a comprender el cómo, donde, y por qué podría ocurrir está perdida, las siguientes etapas recolectan datos de entrada para esta actividad Identificación de riesgos. Normalmente se identifican los riesgos como eventos o situaciones no deseadas que se pretenden evitar, por tal razón la identificación de riesgos inicia con términos como: Ausencia, No adherencia, Inadecuada, No suficiencia, entre otros.

Una vez se identifique el riesgo, debe complementarse para obtener el contexto del riesgo, ya que éste puede presentarse en un área, en un horario, por parte de un grupo de colaboradores, o en unas circunstancias específicas que ayudarán más adelante a determinar las acciones a tomar. Estos son algunos ejemplos de preposiciones a utilizar: al, durante, en, sobre, con, hacia, de, mediante, entre otro.

- *Categorías de riesgos:*

  - ✓ **ET: Estratégicos**: Relacionados a lineamientos, políticas, estrategias o directrices no adecuadas o no convenientes para la Entidad.
  - ✓ **OP: Operativo**: Relacionado a procesos, conductas o actividades inapropiadas, contrarias al deber ser o que presente una posible brecha frente a la calidad esperada.
  - ✓ **FA: Financiero:** Relacionado con la asignación, suficiencia o recaudo de recursos económicos que puedan afectar a corto, mediano o largo plazo financieramente a los procesos o la entidad.
  - ✓ **TEC: Tecnológico**: Relacionado al uso, manejo o disposición de equipos biomédicos, industriales o de cómputo y periféricos.

Descripción de Causas: Se describen las causas asociadas al riesgo identificado, pueden ser intrínsecas: atribuidas a personas, métodos, materiales, equipos, instalaciones, directamente involucradas en el proceso o externas: cuando provienen del entorno en el que se desarrolla el proceso

Análisis: la Calificación y la evaluación del riesgo de Seguridad y Privacidad de la Información, Inherente al proceso.

Consecuencias: Se describen los efectos asociados a la materialización del riesgo, que incidan sobre el objetivo del proceso o la Entidad. Pueden agruparse en: Daños a pacientes o trabajadores, Pérdidas económicas, Perjuicio de la imagen, Sanciones legales, reproceso, Demoras, Insatisfacción, entre otras.

Barreras de Seguridad Existentes o Descripción del tratamiento a seguir: Se describen los controles implementados o barreras que existen actualmente para evitar la materialización del riesgo, se pueden encontrar en los protocolos o procedimientos documentados, en las guías de reacción inmediata o en los correctos de buenas prácticas de seguridad del paciente

Valoración del Riesgo: Se mide en cuanto a probabilidad e impacto para obtener un dato cuantitativo que permita su comparación y priorización, como se muestra en las siguientes escalas de valoración.

Tratamiento y Seguimiento del Riesgo: Se describen los controles o barreras a ser implementadas que fortalezcan las existes, con lo cual aportar y evitar la materialización del riesgo desde la reducción de la probabilidad y/o del impacto. Las acciones propuestas pueden en algunos casos significar actualización de protocolos o procedimientos documentados, adopción de mejores prácticas a través de referenciaciones realizas, fortalecimiento de buenas prácticas de seguridad del paciente, asesorías con expertos, entre otras. Un aspecto de gran importancia es la definición de indicadores para determinar el impacto de las acciones realizadas, ya que no es suficiente cumplir las actividades propuestas sino también valorar como estas acciones permiten disminuir la probabilidad de ocurrencia o nivel de impacto del riesgo; es decir, el indicador mide la efectividad de las acciones frente a la mitigación del riesgo.

6.4 PANORAMA DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN:

RIESGO	FUENTE	CAUSA	CONSECUENCIA	CONTROLES EXISTENTES	RECURSO AFECTADO	EVALUACIÓN DEL RIESGO	DESCRIPCIÓN DEL TRATAMIENTO
ET - Estratégicos	Fuentes Externas El gobierno Entes Reguladores Alta Dirección Tecnología	Una falla en el análisis previo frente a los cambios que se hagan en la E.S.E Hospital San Rafael de Itagüí, de acuerdo con los requerimientos legales aplicables. Ejecutar Inoportuna o Inadecuadamente los lineamientos, políticas, estrategias o directrices no adecuadas o no convenientes para la E.S.E Hospital San Rafael de Itagüí. Divulgación de información confidencial del Hospital San Rafael de Itagüí, sin previa autorización, ni justificación, por parte de los usuarios, personal vinculado, contratistas, agremiados.	Sanciones Y demandas por incumplimientos o implementaciones inadecuadas a la Ley, Normas, Decretos, Resoluciones y Acuerdos Demandas y acciones legales en contra de la E.S.E Hospital San Rafael de Itagüí	Derechos y deberes personal vinculado, contratista, agremiados y usuarios, en guardar la confiabilidad de la información. Aviso de privacidad y protección de la información Política de protección de datos personales.	Buen Nombre de la ESE Financiero Tiempo	Critico	Siempre que se generen requerimientos legales se debe hacer control por medio de un grupo interdisciplinario donde se tengan en cuenta todas las posibles variables de los procesos del Hospital san Rafael de Itagüí Se deben de cumplir a cabalidad los controles establecidos para la protección de la información y datos personales. Auditoria Anual

RIESGO	FUENTE	CAUSA	CONSECUENCIA	CONTROLES EXISTENTES	RECURSO AFECTADO	EVALUACIÓN DEL RIESGO	DESCRIPCIÓN DEL TRATAMIENTO
OP - Operativos	Todo el personal que maneje la información a los funcionarios, a las agremiaciones y los Contratistas de la E.S.E Hospital San Rafael de Itagüí Los Procesos Internos Eventos Externos Tecnología de la Información	Falta de un adecuado adiestramiento La digitalización inadecuada de la Información La oportuna y adecuada clasificación de los documentos para los respaldos de información necesarios para garantizar la protección de la de la Información.	Pedida Parcial o definitiva o información. Demandas y acciones legales en contra de la E.S.E Hospital San Rafael de Itagüí.	Control de ingreso a los equipos y a los aplicativos de TI Política de tratamiento de la información y datos personales.	Tiempo Financiero El Buen Nombre de la E.S.E Hospital San Rafael de Itagüí.	Critico	Capacitación al funcionario, Contratistas y Agremiación en los procesos de la E.S.E Hospital San Rafael de Itagüí. Una Metodología de Respaldo para todos

RIESGO	FUENTE	CAUSA	CONSECUENCIA	CONTROLES EXISTENTES	RECURSO AFECTADO	EVALUACIÓN DEL RIESGO	DESCRIPCIÓN DEL TRATAMIENTO
TEC – Tecnología	Personas responsables del proceso de tecnología y sistemas de la Información Contratistas	Fallas en el en los equipos de Tecnología Controles inadecuados para custodiar la información. Inexactitudes en controles de sistemas para evitar personas indeseadas en la red y perdida de información La realización inadecuada de los respaldos de información necesarios para garantizar la protección de la de los Datos La inadecuada custodia de la Información Física y Digital Fallas Eléctricas en la Instalaciones de la E.S.E Hospital San Rafael de Itagüí.	Perdida de información valiosa del Hospital san Rafael de Itagüí Filtración de información privada o confidencial Demandas y acciones legales en contra de la E.S.E Hospital San Rafael de Itagüí.	Personal competente vinculado al Hospital para atender todas las novedades y brindar soporte tecnológico permanente. Creación de Perfiles y usuarios para los equipos y los aplicativos Un sistema de Cortafuegos Un Aplicativo tipo Antivirus Unidades de UPS, para el Centro de Cómputo. Se cuenta con una planta Eléctrica de ACPM	Financiero Reputacional Buen Nombre de la E.S.E Hospital San Rafael de Itagüí.	Critico .	Realización de los respaldos y pruebas de restauración de la información de forma periódica.

6.5 PROGRAMACION DE ACTIVIDADES:

GESTIÓN	ACTIVIDAD	TAREA	RESPONSABLE	FECHA DE INICIO	FECHA DE FIN
Gestión de Riesgos	Actualización de lineamientos de riesgos	Actualizar política y metodología de gestión de riesgos	Área de sistemas	01/01/2021	31/03/2021
	Sensibilización	Socialización Guía y Herramienta - Gestión de Riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación	Área de sistemas	01/02/2021	30/04/2021
	Identificación de Riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y continuidad de la Operación	Identificación, Análisis y Evaluación de Riesgos - Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación	Área de sistemas	01/02/2021	30/04/2021
		Realimentación, revisión y verificación de los riesgos identificados (Ajustes)	Área de sistemas	01/03/2021	31/05/2021
	Aceptación de Riesgos Identificados	Aceptación, aprobación Riesgos identificados y planes de tratamiento	Área de sistemas	01/06/2021	30/06/2021
	Publicación	Publicación Matriz de riesgos - SIMIG	Área de sistemas	01/07/2021	31/07/2021
	Seguimiento Fase de Tratamiento	Seguimiento estado planes de tratamiento de riesgos identificados y verificación de evidencias	Área de sistemas	01/08/2021	30/11/2021
	Evaluación de riesgos residuales	Evaluación de riesgos residuales	Área de sistemas	01/07/2021	30/09/2021
	Mejoramiento	Identificación de oportunidades de mejora acorde a los resultados obtenidos durante la evaluación de riesgos residuales	Área de sistemas	01/10/2021	31/10/2021
		Actualización Guia Gestión de Riesgos Seguridad de la información, de acuerdo a los cambios solicitados	Área de sistemas	01/08/2021	30/10/2021
	Monitoreo y Revisión	Generación, presentación y reporte de indicadores	Área de sistemas	01/11/2021	30/11/2021

8. PRESUPUESTO

La E.S.E Hospital San Rafael de Itagüí, cuenta con un Presupuesto asignado, para los diferentes procesos de Compras y Mantenimiento.

9. EVALUACIÓN

Para continuar con el análisis y la evaluación del riesgo, este dependerá de la información obtenida en las fases de identificación anteriormente descritas de Identificación de los riesgos, es por lo que la entidad debe crear los criterios de riesgo definiendo los niveles de riesgo aceptado por la Organización. De esta forma la guía menciona cuales son los pasos claves en el análisis de riesgos, probabilidad e impacto, definiendo como sigue cada uno de ellos : “Por Probabilidad se entiende la posibilidad de ocurrencia del riesgo; esta puede ser medida con criterios de Frecuencia, si se ha materializado (por ejemplo: número de veces en un tiempo determinado), o de Factibilidad teniendo en cuenta la presencia de factores internos y externos que pueden propiciar el riesgo, aunque éste no se haya materializado. Por Impacto se entienden las consecuencias que puede ocasionar a la organización la materialización del riesgo”. De esta forma se procede a hacer la “calificación del riesgo”, en la cual se realiza una estimación, de cuál podría ser la probabilidad de ocurrencia del riesgo y el impacto que traería éste, en caso de materializarse. De igual forma la guía presenta una “tabla de probabilidad” y una “Tabla de Impacto”, en las cuales presenta 5 niveles para medir la probabilidad de ocurrencia y 5 niveles para lograr medir el impacto, dando las herramientas con las cuales se definen los criterios de riesgo. Por otro lado, presenta la tabla en la cual se señalan “los impactos de mayor ocurrencia en las Entidades del Estado”, en éste punto se toca el impacto sobre la Confidencialidad de la Información, el cual es uno de los pilares de la Seguridad de la Información.

Impacto Sobre la Confidencialidad de la Información

NIVEL	CONCEPTO
1	Personal
2	Grupo de Trabajo
3	Relativa al Proceso
4	Institucional
5	Estratégica

Fuente: Guía de Riesgos DAFP

Esta se hace de manera cualitativa generando una comparación en la cual se presenta el análisis de la probabilidad de ocurrencia del riesgo versus el impacto del mismo, obteniendo al final la matriz denominada “Matriz de Calificación, Evaluación y respuesta a los Riesgos”, con la cual la guía presenta la forma de calificar los riesgos con los niveles de impacto y probabilidad establecidos anteriormente, así como las zonas de riesgo presentando las posibles formas de tratamiento que se le puede dar a ese riesgo, tal como se muestra en la siguiente imagen

Ilustración 3 “Matriz de Calificación, Evaluación y respuesta a los Riesgos”

PROBABILIDAD	IMPACTO				
	Insignificante (1)	Menor (2)	Moderado (3)	Mayor (4)	Catastrófico (5)
Raro (1)	B	B	M	A	A
Improbable (2)	B	B	M	A	E
Posible (3)	B	M	A	E	E
Probable (4)	M	A	A	E	E
Casi Seguro (5)	A	A	E	E	E

B: Zona de riesgo Baja: Asumir el riesgo
M: Zona de riesgo *Moderada:* Asumir el riesgo, Reducir el riesgo
A: Zona de riesgo *Alta*: Reducir el riesgo, Evitar, Compartir o Transferir
E: Zona de riesgo *Extrema*: Reducir el riesgo, Evitar, Compartir o Transferir

Fuente: Guía de Riesgos DAFP

Una vez se cumpla con las actividades programadas para la identificación y creación de la matriz de riesgos, se tendrá en cuenta la guía de tratamiento de riesgos de seguridad y privacidad de la información, donde no solo se obtendrán los riesgos a intervenir, sino que se crearan estrategias para el tratamiento de los mismos basados en las 4 opciones que nos ofrece la guía como lo son trasferir, mitigar, evitar o aceptar, sea un riesgo interno o externo, además, de realizar una evaluación, seguimiento y monitoreo de los mismos, utilizando los recursos humanos y físicos con los que cuenta la E.S.E. Hospital San Rafael de Itagüí.

DIEGO LEON MUÑOZ ZAPATA
Gerente E.S.E Hospital San Rafael de Itagüí.