HOSPITAL DEL SARARE
Empresa Social del Estado

Plan de Tratamiento de Riesgos y Privacidad de la Información

Sistema Integrado de Gestión

Subproceso Gestión de las Tics.

WWW.HOSPITALDELSARARE.GOV.CO

Evolucionamos pensando en Usted

CONTENIDO

INTRODUCCION

El plan de tratamiento de riesgos de Seguridad y Privacidad de la información, Seguridad Digital en el Hospital del Sarare, 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, y teniendo como orientación los lineamientos y buenas practicas establecidas en la ISO 27001:2013 e ISO 31000:2018, el hospital del Sarare adopota la Guía para la administración del riesgo y el diseño de controles en entidades públicas (Dic 2020) - Riesgos de gestión, corrupción y seguridad digital - Versión 4 emitida por el Departamento Administrativo de la Funciona Pública DAFP y aquellas que él Hospital defina.

1. OBJETIVO.

Establecer las acciones específicas y metodología para la administración de los riesgos del Modelo de seguridad y privacidad de la Información del Hospital del Sarare E.S.E, a partir de su identificación, evaluación, tratamiento y seguimiento con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de la información.

2. ALCANCE.

Será aplicable a todos los procesos estratégicos, misionales, de apoyo y a terceros que creen, procesen, transmitan o resguarden información de nuestros usuarios durante la vigencia 2022**.**

3. DEFINICIONES.

- **Amenaza:** es un ente o escenario interno o externo que puede hacer uso de una vulnerabilidad para generar un perjuicio o impacto negativo en la institución (materializar el riesgo).

- **Análisis de Riesgo**: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).

- **Auditoría:** Proceso sistemático, independiente y documentado para obtener evidencias de auditoria y obviamente para determinar el grado en el que se cumplen los criterios de auditoria. (ISO/IEC 27000).

- **Activos de información:** Elementos de Hardware y de Software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de cada entidad, órgano u organismo.

  Este tipo de activo representa los datos de la organización, información que tiene valor para los procesos de negocio, independientemente de su ubicación: puede ser un documento físico debidamente firmado, un archivo guardado en un servidor, un aplicativo o cualquier elemento que permita almacenar información valiosa o útil para el Hospital del Sarare.

- **Confidencialidad**: Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

- **Control:** Es toda actividad o procesos encaminados a prevenir, mitigar o evitar un riesgo. Incluye políticas, procedimientos, guías, estructuras organizacionales, buenas prácticas que pueden ser de carácter administrativo, técnico o legal.

- **Disponibilidad**: Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.

- **Evento de seguridad de la información**: Se considera un Evento de Seguridad de la Información a cualquier situación identificada que indique una posible brecha en la Política de Información o falla en los controles y/o protecciones establecidas.

- **Impacto:** son las consecuencias que genera un riesgo una vez se materialice.

- **Incidente de seguridad de la información:** Un incidente de seguridad de la información se define como un acceso, uso, divulgación, modificación o destrucción no autorizada de la información y de sus usuarios; un impedimento en la operación normal de las redes, sistemas o recursos informáticos; o cualquier otro acto que implique una violación a la Política de Información.

- **Información:** Información almacenada o procesada física o digitalmente " Bases de datos, archivos de datos, contratos, acuerdos, documentación del sistema, información sobre investigación, manuales de usuario, material de formación o capacitación, procedimientos operativos o de soporte, planes para la continuidad del negocio, acuerdos de recuperación, registros de auditoria e información archivada).

- **Integridad:** Propiedad de salvaguardar la exactitud y estado completo de los activos.

- **Probabilidad:** es la posibilidad de la amenaza aproveche la vulnerabilidad para materializar el riesgo.

- **Propietario/responsable de activo de información**: Individuo, entidad o unidad de negocio que ha aceptado la responsabilidad de la administración para el control, producción, desarrollo, mantenimiento, uso y seguridad de los activos de información.

- **Seguridad de la Información**: Este principio busca crear condiciones de uso confiable en el entorno digital, mediante un enfoque basado en la gestión de riesgos, preservando la confidencialidad, integridad y disponibilidad de la información de las entidades del Estado, y de los servicios que prestan al ciudadano.

- **Servicio:** Es cualquier acto o desempeño que una persona puede ofrecer a otra que es esencialmente intangible y que no conlleva ninguna propiedad. Su producción puede o no estar ligada a un producto físico.

- **Usuario:** Es el nombre (o alias) que se le asigna a cada persona para ser identificado por el servidor, de esta manera el proveedor de Internet o de correo electrónico lo identifica, es única en cada servidor, y cada usuario tiene asignado una contraseña para poder acceder a su cuenta.

- **Riesgo:** es un escenario bajo el cual una amenaza puede explotar una vulnerabilidad generando un impacto negativo al negocio evitando cumplir con sus objetivos.

- **Riesgo de seguridad de la información:** Posibilidad de que una amenaza concreta que pueda aprovechar una vulnerabilidad para causar una pérdida o daño en un activo de información; estos daños consisten en la afectación de la confidencialidad, integridad o disponibilidad de la información. Cuando la amenaza se convierta en una oportunidad se debe tener en cuenta en el beneficio que se genera.

- **Vulnerabilidad:** es una falencia o debilidad que puede estar presente en la tecnología, las personas o en las políticas y procedimientos.

4. DESARROLLO METODOLOGICO

Se requiere prevenir y reducir los efectos indeseados a la hora de materializarse un riesgo que afecte un activo de la información, procurar la mejora continua, definir acciones para tratar los riesgos de seguridad de la información y evaluar la eficacia de las acciones tomadas; el Hospital del Sarare E.S.E identificará y clasificará los activos de la información, los riesgos de seguridad de la información y definirá las acciones a tomar bajo los lineamientos definidos por MINTIC y los establecidos en el Manual de administración de los riesgos DIR-00-M03 del Hospital del Sarare E.S.E y de acuerdo al Sistema de la información y privacidad de la Información.

4.1 POLITICA DE ADMINISTRACIÓN DEL RIESGO

La alta dirección mediante muestra su compromiso con la gestión y control de los riesgos mediante la resolución 259 del 23 de noviembre del 2017 la cual adopta la política la política de administración del riesgo en el Hospital del Sarare E.S.E. la cual puede ser consultada en la página web en la sección de políticas; http://www.hospitaldelsarare.gov.co/publicaciones/normas,-procedimientos-y-lineamientos/politicas.html

4.2 ADMINISTRACIÓN DE LOS RIESGOS

La administración de los riesgos se realizará bajo los lineamientos definidos Hospital del Sarare E.S.E en sus políticas; administración de los riesgos, gobierno digital, seguridad digital, seguridad informática, tratamiento de datos, trasparencia y acceso a la información, y se realizará de acuerdo a lo establecido en el **Manual de administración de los riesgos DIR-00-M03** el cual adopta la metodología de propuesta por el DAFP (2020) Guía de administra del riesgo y el diseño de controles en entidades públicas.

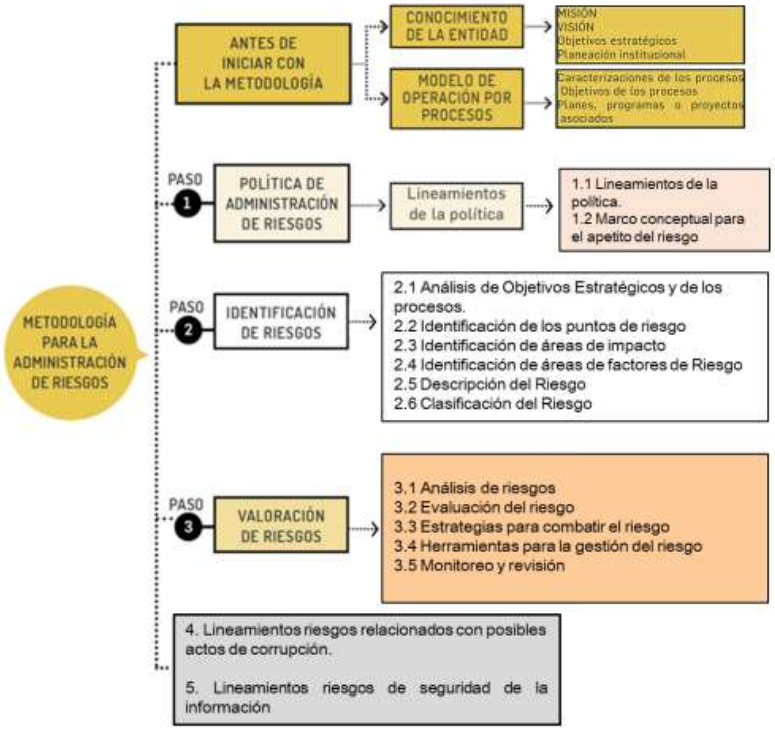

Ilustración 2: Modelo de administración del riesgo
Fuente: Guía de administra del riesgo y el diseño de controles en entidades públicas.

La administración de los riesgos asociados a la seguridad de la información se realizará en todos y cada uno de los procesos estratégicos, misionales, apoyo, control y seguimiento del Hospital del Sarare E.S.E mediante la construcción del Mapa de riesgos del proceso/subproceso que integrado los riesgos de seguridad de la información y la determinación de los respectivos planes de mejoramiento.

4.3 IDENTIFICACIÓN DEL RIESGO

En esta etapa se espera que los líderes de procesos identifiquen los riesgos bajo los cuales se tiene control o no y están asociados a sus procesos/subprocesos de acuerdo al análisis del entorno y contexto estratégico, la caracterización del proceso/subproceso, los objetivos y metas definidos y bajo el modelo de operación por procesos del Hospital del Sarare E.S.E y a su vez generan riesgos para el logro de los objetivos institucionales.

4.4 IMPLEMENTACIÓN

4.2.1 EJECUCIÓN DEL PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Ejecutar el plan de tratamiento de los riesgos transversales de seguridad de la información identificados en la fase de planificación que fue presentado en el comité de gestión y desempeño.

4.3 EVALUACIÓN DEL DESEMPEÑO

El plan de tratamiento de riesgos de Seguridad y privacidad de la información forma parte integral del modelo de seguridad y privacidad de la información MSPI y todas las actividades de seguimiento, medición, análisis, auditoria y revisión por la dirección se realizará de acuerdo a lo definido en el plan de seguridad y privacidad de la información.

5. BIBLIOGRAFÍA.

ISO/IEC 27001:2013
Modelo de Privacidad y Seguridad de la información del MINTIC
Guía 7: gestión del Riesgo de MINTIC
Guía 5: Gestión y clasificación de los activos de MINTIC

6. CONTROL DE CAMBIOS

REVISIÓN N°	FECHA DE APROBACIÓN DD/MM/AA	DESCRIPCIÓN DE CAMBIOS
00	17-12-2021	Creación del Documento 17-12-2021
	-	