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

INTRODUCCIÓN

El plan de tratamiento de riesgos de Seguridad y Privacidad de la información, se basa en una orientación estratégica que requiere el desarrollo de una cultura de carácter preventivo, de manera que, al comprender el concepto de riesgo, así como el contexto, se planean acciones que reduzcan la afectación a la entidad en caso de materialización, adicional se busca desarrollar estrategias para la identificación, análisis, tratamiento, evaluación y monitoreo de dichos riesgos y desarrollar controles que permitan minimizar y fortalecer la seguridad de los sistemas de información y de su infraestructura.

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 de los estándares ISO 27001:2013, 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 DAFP.

DEFINICIONES

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

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).

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

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

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

Control o Medida: acciones o mecanismos definidos para prevenir o reducir el impacto de los

eventos que ponen en riesgo, la adecuada ejecución de las actividades y tareas requeridas para el logro de objetivos de los procesos de una entidad.

Controles: Procesos, políticas y/o actividades que pueden modificar el riesgo.

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.).

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.

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 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

OBJETIVO

Incluir en la gestión de riesgos institucionales la identificación y análisis de los riesgos relacionados con la seguridad de la información.

OBJETIVOS ESPECIFICOS

- Definir la metodología y etapas de implementación
- Realizar el plan de trabajo para la implementación
- Identificar los riesgos actuales, las posibles causas y los controles existentes.

ALCANCE DEL DOCUMENTO

Realizar una eficiente gestión de riesgos de Seguridad y Privacidad de la Información de la entidad, que permita integrar en los procesos de la entidad buenas practicas que contribuyan a la toma de decisiones y prevenir incidentes que afecten los objetivos de la entidad.

MARCO NORMATIVO

NORMATIVIDAD	CONTENIDO
CONPES 3854 de 2016	Política Nacional de Seguridad Digital
Norma internacional ISO 31000:2018	Sistemas de gestión del riego
Norma internacional ISO 27000:2013	Seguridad de la información
Ley Estatutaria 1581 de 2012	Protección de datos personales
Ley 1266 de 2008	Disposiciones generales de habeas data y se regula el manejo de la información
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 octubre 2020
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 - MSP	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
Decreto 767 de 2022	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.
Decreto 88 de 2022	Por el cual se adiciona el Título 20 a la Parte 2 del Libro 2 del Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, Decreto 1078 de 2015, para reglamentar los artículos 3, 5 Y 6 de la Ley 2052 de 2020, estableciendo los conceptos, lineamientos, plazos y condiciones para la digitalización y automatización de trámites y su realización en línea
Decreto 338 de 2022	Por el cual se adiciona el Titulo 21 a la parte 2 del libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones

METODOLOGIA

Para la implementación el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información de la entidad el hospital se acoge el modelo del Ministerio de Tecnologías de la Información y las Comunicaciones (Min-TIC), para estar acorde con las buenas prácticas de seguridad y teniendo en cuenta las normas ISO 27001 del 2013, y siguiendo las recomendaciones de la Guía de Gestión de Riesgos de Seguridad y Privacidad de la Información (MINTIC:2016).

Gestión de Riesgos			
Actividad	**Tarea**	**Responsable**	**Fechas**
Actualizar los Lineamientos de riesgos	Actualizar políticas y metodologías de gestión de riesgos	Oficina de Sistemas	Febrero-Marzo
Sensibilización	Socializar la Guía y herramientas de gestión de Riesgos de privacidad y seguridad de la información	Oficina de Sistemas	Abril-Mayo
Identificar Riesgos de privacidad y seguridad de la información	Identificar Riesgos de privacidad y seguridad de la información	Oficina de Sistemas	Abril-Mayo
Aceptación de Riesgos Identificados	Aceptación, aprobación de Riesgos Identificados y planes de tratamiento	Comité de Gestión y Desempeño	Mayo
Publicación	Publicación de Matriz de Riesgos	Comité de Gestión y Desempeño	Mayo
Sensibilización Personal	Realizar actividades de sensibilización de los riesgos de seguridad y privacidad de la información, para el	Oficina de Sistemas	Jul-Dic
Seguimiento	Seguimiento estado de planes de tratamiento de riesgos identificados y verificación de evidencias	Comité de Gestión y Desempeño	Julio-Sep-Dic
Evaluación de Riesgos Residuales	Evaluación de Riesgos Residuales	Comité de Gestión y Desempeño	Julio-Sep-Dic
Mejoramiento	Identificación de Oportunidades de Mejora, acorde a los resultados obtenidos durante la evaluación de los riesgos	Comité de Gestión y Desempeño	Julio-Sep-Dic
Monitoreo y Revisión	Generación, presentación y reportes de indicadores	Comité de Gestión y Desempeño	Julio-Sep-Dic

Desarrollo

Análisis de la Información

En esta etapa se evaluarán los resultados de las entrevistas con los colaboradores del proceso de TI, se desarrollarán las siguientes actividades:

- Aplicar las políticas de tratamiento de riesgos.
- Determinar los controles (se desprenden de las medidas) aplicados en el Ministerio TIC.

- Determinar los riesgos que van a ser incluidos en el Plan de Tratamiento de Riesgos.

Desarrollo de los proyectos (acciones a realizar)

En esta fase se realizarán las actividades que permitan la estructuración de las acciones a realizar.

- Determinar el nombre de las acciones a realizar.
- Definir los responsables de cada acción.
- Establecer el objetivo de cada acción.
- Elaborar la justificación de la acción.
- Definir las actividades a realizar para el desarrollo de la acción.

Análisis de los proyectos

- Definición de los controles relacionados con cada acción.
- Validar los riesgos mitigados por cada acción.
- Análisis de la aplicabilidad de las acciones.
- Priorización de las acciones.

Definición del organigrama de responsabilidad

En esta fase se realizará un organigrama y se definirán responsabilidades respecto a la administración y gestión del riesgo, esta etapa deberá ser definida por el Hospital teniendo en cuenta su estructura organizacional para la gestión de riesgos.

- Definición del grupo de trabajo de gestión de riesgo por parte del Hospital.
- Definición de las funciones del grupo de trabajo referentes a la aplicación y gestión de las acciones.

Ciclo de vida del tratamiento de riesgos

La gestión del riesgo dentro de la seguridad de la información se puede también enmarcar dentro el ciclo de planear, hacer, verificar y actual(PHVA) tal como se muestra en la ilustración (ISO 27001:2013).

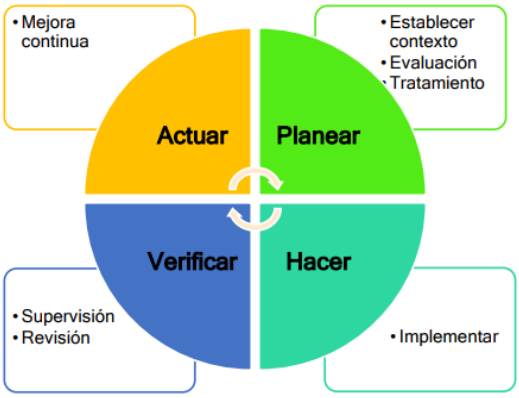

Ilustración 2. Ciclo PHVA y la gestión de riesgos

Planear: Dentro de esta etapa se desarrollan las actividades definidas en la fase 1 de la metodología de tratamiento de riesgos.

Hacer: En este paso del ciclo de vida se desarrollarán las actividades enmarcadas en la fase 2 de la metodología del tratamiento de riesgos.

Verificar: En esta etapa se desarrollarán las actividades que permiten hacer seguimiento o auditorías a la ejecución de cada una de las medidas.

Actuar: Dentro de esta etapa se realizarán las mejoras teniendo en cuenta el seguimiento y los resultados de las auditorías de la ejecución de los proyectos.

RECURSOS

RECURSOS	VARIABLES
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
Tecnicos	Guía de 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)
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

MEDICIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La medición se realiza con un indicador de gestión que está orientada principalmente en la medición de eficacia de los componentes de implementación y gestión definidos en el modelo de operación del marco de seguridad y privacidad de la información. que servirán como insumo para el componente de mejora continua permitiendo adoptar decisiones de mejora sobre Seguridad de la información.

MEDICIÓN La medición se realiza con un indicador de gestión que está orientado principalmente a determinar el porcentaje de implementación de los controles definidos en el tratamiento de riesgos de seguridad y privacidad de la información.