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

Hospital San Rafael Empresa Social del estado

El Águila, Valle del Cauca

Año 2023.

Tabla de contenido

1. PLAN TRATAMIENTO DE RIESGO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información establece las actividades requeridas para la gestión de los riesgos de seguridad y privacidad de la información, en función de la implementación de controles que permitan a la entidad disminuir la probabilidad y el impacto de materialización de este tipo de riesgos, con el fin de preservar la seguridad e integridad de los activos de información de la Entidad. En este sentido, acorde con lo establecido en el Modelo de Seguridad y Privacidad de la Información – MSPI, en la Guía No. 7 – Guía de Gestión de Riesgos y Guía No. 8 – Controles de Seguridad y Privacidad de la Información, en el presente Plan se estipulan directrices, fechas de ejecución y responsables para lograr un adecuado proceso de administración y evaluación de los riesgos de seguridad y privacidad de la información.

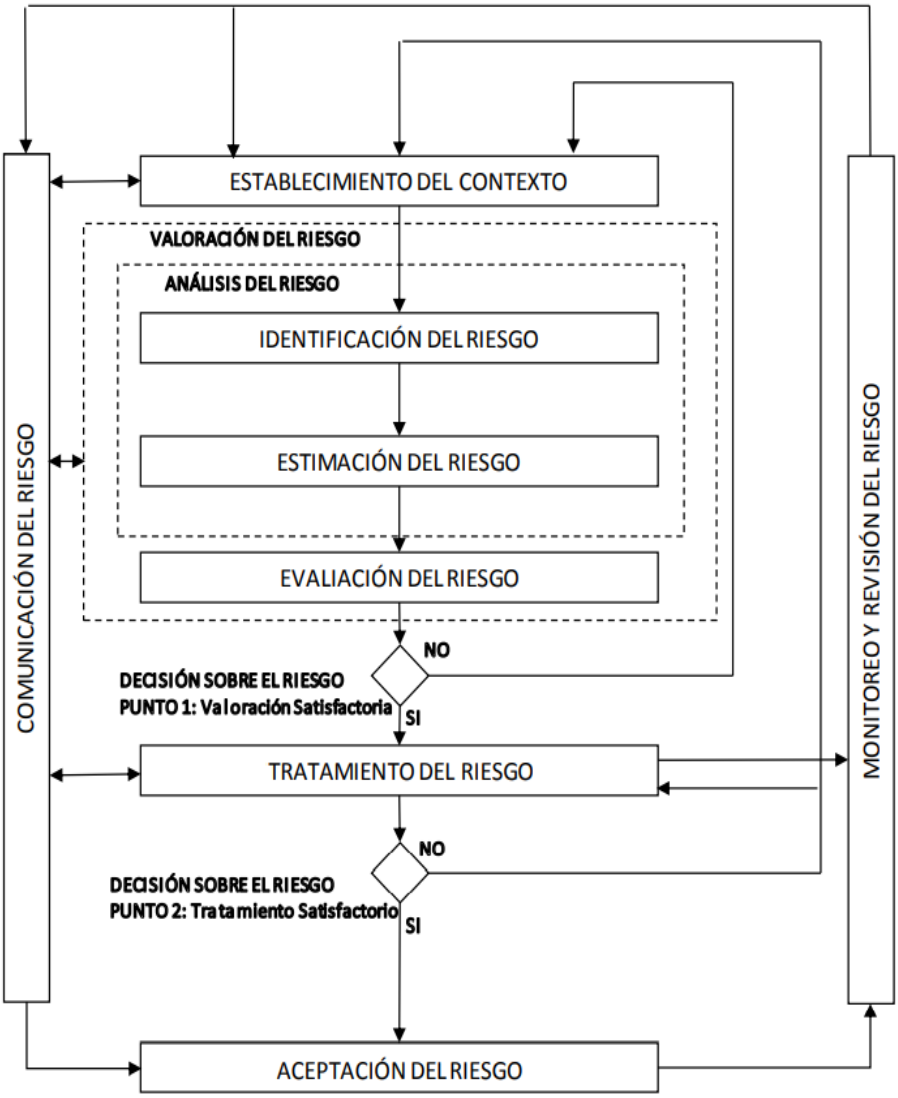
Objetivo.

Desarrollar e implementar el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, de acuerdo con lo establecido en el Modelo de Privacidad y Seguridad de la Información – MSPI, la Guía No. 7 – Guía de Gestión de Riesgos y la Guía No. 8 – Controles de Seguridad y Privacidad de la Información, con el propósito de adoptar medidas y acciones encaminadas a modificar, reducir o eliminar riesgos relacionados con la infraestructura de tecnologías de la Información del Hospital San Rafael Empresa Social del Estado, del municipio de El Águila, Valle del Cauca.

Alcance

Los requisitos, lineamientos y acciones establecidas en el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información son aplicables de forma anualizada a los procesos estratégicos, misionales, de apoyo y de evaluación, por lo cual deberán ser conocidos y cumplidos por todos los funcionarios, contratistas, recursos de infraestructura tecnológica para el tratamiento de la información y terceras partes vinculadas a la Entidad que accedan a los activos de información, sistemas de información e instalaciones físicas del Hospital San Rafael Empresa Social del Estado.

2. PROCESO PARA EL TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.



lustración 1. Proceso para la administración de riesgos de seguridad y privacidad de la información
Fuente: https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf

Para la evaluación de riesgos de seguridad y privacidad de la información se tomará como insumo la matriz de Activos de Información, sobre la cual se implementará el presente Plan sobre los Activos de Información que tengan un nivel alto de clasificación al evaluar los criterios de confidencialidad, integridad y disponibilidad, según los siguientes criterios

CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
INFORMACIÓN PUBLICA RESERVADA	ALTA (A)	ALTA (1)
INFORMACIÓN PUBLICA CLASIFICADA	MEDIA (M)	MEDIA (2)
INFORMACIÓN PÚBLICA	BAJA (B)	BAJA (3)
NO CLASIFICADA	NO CLASIFICADA	NO CLASIFICADA

Ilustración 2. Criterios de Clasificación
Fuente: https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf

ALTA	Activos de información en los cuales la clasificación de la información en dos (2) o todas las propiedades (confidencialidad, integridad, y disponibilidad) es alta.
MEDIA	Activos de información en los cuales la clasificación de la información es alta en una (1) de sus propiedades o al menos una de ellas es de nivel medio.
BAJA	Activos de información en los cuales la clasificación de la información en todos sus niveles es baja.

Ilustración 3. Niveles de Clasificación
Fuente: https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf

3. CRONOGRAMA PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

A continuación, cronograma propuesto para la implementación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información en la Entidad y descripción general de las tareas principales.

ID	ACTIVIDAD	FECHA INICIO	FECHA FINAL
1	Sensibilización Institucional sobre política de seguridad de la información	01/02/2023	30/12/2023
2	Desarrollar y/o actualizar el inventario de activos de información.	01/02/2023	30/06/2023
3	Elaborar procedimientos gestión de riesgos de seguridad de la información	01/02/2023	30/06/2023
4	Definir metodología para la gestión de los riesgos de seguridad y privacidad de la información	01/07/2023	30/12/2023
5	Definir herramienta de análisis de Riesgo de seguridad de la información para la implementación del riesgo	01/07/2023	30/12/2023
6	Ejecutar Plan de riesgos de seguridad y privacidad de la información	01/02/2023	30/12/2023

3.1. Sensibilización institucional sobre política de seguridad de la información

Realizar la divulgación de manera apropiada de las reglas de comportamiento adecuadas para el uso de los sistemas y la información, que generalmente están plasmadas en las políticas y procedimientos de seguridad de la información que la Entidad requiere que sean cumplidos por parte de todos los usuarios del sistema. Cualquier incumplimiento a las políticas, debe llevar a la imposición de una sanción, siempre y cuando el usuario haya sido adecuadamente capacitado e informado sobre todo el contenido de seguridad correspondiente a su rol y responsabilidades dentro de la Entidad.

3.2. Actualizar el inventario de activos de información

Se desarrollará una metodología para la identificación, clasificación, mantenimiento y actualización del inventario de activos de información, entendiendo que hace parte de la debida diligencia que a nivel estratégico se ha definido en el Modelo de Seguridad y Privacidad de la Información. En concordancia, el inventario de activos de la información se registra en la matriz definida por la Entidad incluyendo la información pertinente respecto a los propietarios, custodios y usuarios de los activos de información identificados en cada vigencia.

3.3. Elaborar procedimientos de seguridad de la información.

Se realizará la revisión de los actuales procedimientos, con el objeto de identificar las necesidades de documentación y/o actualización de procedimientos en el marco de la implementación del Modelo de Seguridad y Privacidad de la información. El propósito de esta actividad se fundamenta en desarrollar y formalizar procedimientos que permitan gestionar la seguridad y privacidad de la información en todos los procesos de la Entidad.

3.4. Definir metodología para la gestión de los riesgos de seguridad y privacidad de la información.

Se definirá una metodología de gestión del riesgo enfocada a procesos, que le permita identificar, evaluar, tratar y dar seguimiento a los riesgos de seguridad de la información a los que estén expuestos los activos, así, como la declaración de aplicabilidad. Para conseguir una integración adecuada entre el MSPI y la guía de gestión del riesgo emitida por el DAFP respecto a este procedimiento, se recomienda emplear los criterios de evaluación (impacto y probabilidad) y niveles de riesgo emitidos por esta entidad.

3.5. Definir herramienta del análisis de Riesgo de seguridad de la información para la implementación del riesgo.

Se definirá la herramienta de gestión del riesgo enfocada a procesos, que le permite localizar y visualizar los recursos de la entidad que se encuentran más en peligro de sufrir daño por algún impacto negativo, para posteriormente ser capaz de tomar decisiones y medidas adecuadas para la reducción de amenazas.

3.6. Ejecutar plan de riesgos de seguridad y privacidad de la información

ID	TAREAS PRINCIPALES	F. INICIO	F. FINAL
6.1	Definir el contexto estratégico	01/02/2023	30/07/2023
6.2	Establecer equipo de trabajo con asignación responsabilidades	01/02/2023	30/07/2023
6.3	Identificación de riesgos	01/03/2023	30/08/2023
6.4	Análisis de riesgos	01/04/2023	30/09/2023
6.5	Valoración de riesgos	01/05/2023	30/10/2023
6.6	Evaluación de controles	01/06/2023	30/11/2023
6.7	Socialización y comunicación políticas de riesgos	01/07/2023	30/12/2023
6.8	Monitoreo y revisión al tratamiento de los riesgos	permanente	

3.6.1. Establecer contexto estratégico

Definir el contexto estratégico contribuye al control de la entidad frente a la exposición al riesgo, ya que permite conocer las situaciones generadoras de riesgos, impidiendo con ello que la entidad actúe en dirección contraria a sus propósitos institucionales.

Para la definición del contexto estratégico, es fundamental tener claridad de la misión institucional, sus objetivos y tener una visión sistémica de la gestión, de manera que se perciba la administración del riesgo como una herramienta gerencial y no como algo aislado del accionar administrativo. Por lo tanto, el diseño de esta

primera etapa, se fundamenta en la identificación de los factores internos (debilidades) y externos (amenazas) que puedan generar riesgos que afecten el cumplimiento de los objetivos institucionales.

Esta etapa es orientadora, se centra en determinar las amenazas y debilidades de la entidad; es la base para la identificación del riesgo, dado que de su análisis suministrará la información sobre las CAUSAS del riesgo.

3.6.2. Establecer equipo de trabajo con asignación responsabilidades

Tomando como referente lo anterior, se debe atender y seguir las siguientes orientaciones:

- Cada responsable de proceso del Sistema Integrado de Gestión, deberá identificar a los funcionarios que por su competencia pueden ser considerados claves dentro de cada una de las dependencias que participan en el proceso, serán factores de selección de estos, el conocimiento y nivel de toma de decisiones sobre el proceso.
- Los funcionarios seleccionados deberán ser convocados a una reunión inicial, en donde se presentará el propósito de esta actividad.

3.6.3. Identificación de Riesgos

Es la etapa que permite conocer los eventos potenciales, estén o no bajo el control de la entidad pública, que ponen en riesgo el logro de su misión, estableciendo las causas y consecuencias de la ocurrencia del riesgo.

3.6.4. Análisis de Riesgos

El análisis del riesgo busca establecer la probabilidad de ocurrencia del mismo y sus consecuencias, calificándolos y evaluándolos con el fin de obtener información para establecer el nivel de riesgo.

Se han establecido dos aspectos a tener en cuenta en el análisis de los riesgos identificados, probabilidad e impacto. Por la primera se entiende la posibilidad de ocurrencia del riesgo; esta puede ser medida con criterios de Frecuencia, si se ha materializado, 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 entiende las consecuencias que puede ocasionar a la Entidad la materialización del riesgo.

3.6.5. Valoración de Riesgos

Es el producto de confrontar la evaluación del riesgo y los controles (preventivos o correctivos) de los procesos. La valoración del riesgo se realiza en tres momentos: primero, identificando los controles (preventivos o correctivos) que pueden disminuir la probabilidad de ocurrencia o el impacto del riesgo; luego, se deben evaluar los controles, y finalmente, con base en los resultados de la evaluación de los controles,

determinar la evaluación del riesgo residual y definir la opción de manejo del riesgo. Lo anterior de acuerdo con los formatos Identificación y evaluación de controles y Valoración del riesgo.

3.6.6. Evaluación de Controles

Permite determinar en qué medida los controles identificados están aportando para disminuir los niveles de probabilidad e impacto del riesgo. Se evalúan verificando su documentación, aplicación y efectividad.

3.6.7. Socialización y Comunicación Políticas de Riesgos

Actividad mediante el cual se da conocer a funcionarios, contratistas y terceros de la Entidad las políticas de tratamiento de riesgos de Seguridad y Privacidad de la Información, mediante charlas y el uso de las herramientas de comunicaciones disponibles en la Entidad.

3.6.8. Monitoreo y Revisión al Tratamiento de los Riegos

El monitoreo y revisión debe asegurar que las acciones establecidas en los mapas de riesgo se están llevando a cabo y evaluar la eficacia en su implementación, adelantando revisiones sobre la marcha para evidenciar todas aquellas situaciones o factores que pueden influir en la aplicación de acciones preventivas

3.6.9. Normatividad.

NORMA	EPÍGRAFE DE LA NORMA
Ley 1341 de 2009	Definen Principios y conceptos sobre la sociedad de la información y la organización de las Tecnología e Información y las Comunicaciones - TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones.
CONPES 3701 de 2011	Lineamientos de Política para Ciberseguridad y Ciberdefensa.
Ley 1581 de 2012	Disposiciones generales para la protección de datos personales.
Decreto 1078 de 2015	Decreto único reglamentario del sector de Tecnología e Información y las comunicaciones (define el componente de seguridad y privacidad de la información)
Decreto 415 de 2016	Por el cual se adiciona el Decreto Único Reglamentario del sector de la Función Pública, Decreto número 1083 de 2015, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de Tecnologías de la Información y las Comunicaciones.
CONPES 3854 de 2017	Política Nacional de Seguridad Digital.

Decreto 1499 de 2017, capitulo 2.	Modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública.
CONPES 3920 de 2018.	Política Nacional de Explotación de datos.
	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 Tecnología e Información y las Comunicaciones.
Ley 1978 de 2019.	Moderniza el sector de las Tecnología e Información y las Comunicaciones (TIC), distribuye competencias, crea un regulador único y dicta otras disposiciones.

Carlos A Tapias S.

CARLOS ARTURO TAPIAS SALAZAR
Gerente.