PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION, TRATAMIENTO DE RIESGOS

	ACTUALIZÓ	REVISÓ	APROBÓ
FIRMA:			
NOMBRE:	**FERNANDO CELIS CLAROS**	**María Elvira Yagüe Hurtado**	**Oriana Sofía Peña Mazabel**
CARGO:	Líder Gestión de las Tecnologías	Subdirectora Administrativa y Financiera	Gerente
FECHA:	19/01/2022	19/01/2022	19/01/2022

Contenido

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

INTRODUCCION

En el proceso de implementación del modelo Institucional de Gestión y desempeño MIPG trae consigo una modernización del Estado Colombiano buscando como fin el mejoramiento en la prestación de servicios públicos para el pueblo, mejorando la calidad de vida de los ciudadanos en cada región.

La ESE MANUEL CASTRO TOVAR es una Entidad descentralizada del nivel territorial responsable de la prestación de servicios de salud de primer nivel de atención en la ciudad de Pitalito, por tanto, desarrolla la implementación de MIPG y en consecuencia los productos asociados a este modelo, uno de ellos es el PETI y los planes de seguridad y privacidad de la información y de tratamiento de riesgos de seguridad y privacidad de la información pertenecientes a la política de Gobierno digital.

En este aparte la ESE trabajara conjuntamente los planes de seguridad y privacidad de la información y lo articulara con el PETI.

La ESE es una entidad que apenas en este periodo está trabajando en la migración a la ejecución de actividades misionales haciendo uso de las tecnologías de la información desde sus procesos de planeación estratégica.

El Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC, es la ESE Manuel Castro Tovar encargada de diseñar, adoptar y promover las políticas, planes, programas y proyectos del sector de las Tecnologías de la Información y las Comunicaciones.

La estrategia de Gobierno en Línea, liderada por el Ministerio TIC, tiene como objetivo, garantizar el máximo aprovechamiento de las tecnologías de la información y las comunicaciones, con el fin de contribuir con la construcción de un Estado más participativo, más eficiente y más transparente. La planificación e implementación del Modelo de Seguridad y Privacidad de la Información – MSPI, en la ESE Manuel Castro Tovar está determinado por las necesidades y objetivos, los requisitos de seguridad, los procesos misionales y el tamaño y estructura de la ESE Manuel Castro Tovar.

El Modelo de Seguridad y Privacidad de la Información – MSPI, conduce a la preservación de la confidencialidad, integridad, disponibilidad de la información, permitiendo garantizar la privacidad de los datos, mediante la aplicación de un proceso de gestión del riesgo, brindando confianza a las partes interesadas acerca de la adecuada gestión de riesgos.

A través del decreto único reglamentario 1078 de 2015, del sector de Tecnologías de Información y las Comunicaciones, se define el componente de seguridad y privacidad de la información, como parte integral de la estrategia GEL.

El Modelo de Seguridad y Privacidad de la Información se encuentra alineado con el Marco de Referencia de Arquitectura TI y soporta transversalmente los otros componentes de la Estrategia GEL: TIC para Servicios, TIC para Gobierno Abierto y TIC para Gestión.

OBJETIVOS

Objetivo general

Definir el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información para la ESE Manuel Castro Tovar.

Objetivos específicos

- Lograr un diagnóstico real de la situación actual de la institución en materia de riesgos de seguridad y privacidad de la Información
- Involucrar Funcionarios, Colaboradores y Terceros en la formulación e implementación de controles y acciones encaminadas a prevenir y administrar los riesgos de seguridad y privacidad de información.
- Aportar una base confiable para la toma de decisiones y la planificación institucional en cuanto a la información que se maneja.

ALCANCE

En este documento se define la metodología establecida por la ESE Manuel Castro Tovar para la administración y gestión de los riesgos a nivel de procesos; orienta sobre las actividades a desarrollar desde en cuanto a la identificación de los riesgos, su análisis, valoración, seguimiento y planes de mejora y aplica a todos los procesos de la institución los cuales manejen, procesen o interactúen con la información manejada en la institución.

DEFINICIONES

- **Amenaza:** situación externa que no controla la ESE Manuel Castro Tovar y que puede afectar su operación
- **Análisis del riesgo:** etapa de la administración del riesgo, donde se establece la probabilidad de ocurrencia y el impacto del riesgo antes de determinar los controles (análisis del riesgo inherente).
- **Causa:** medios, circunstancias y/o agentes que generan riesgos.
- **Calificación del riesgo:** estimación de la probabilidad de ocurrencia del riesgo y el impacto que puede causar su materialización.
- **Consecuencia:** efectos que se pueden presentar cuando un riesgo se materializa.
- **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.
- **Debilidad:** situación interna que la ESE Manuel Castro Tovar puede controlar y que puede afectar su operación.
- **Frecuencia:** ocurrencia de un evento expresado como la cantidad de veces que ha ocurrido un evento en un tiempo dado.
- **Impacto:** medida para estimar cuantitativa y cualitativamente el posible efecto de la materialización del riesgo.
- **Mapa de riesgos:** documento que de manera sistemática, muestra el desarrollo de las etapas de la administración del riesgo.
- **Materialización del riesgo:** ocurrencia del riesgo identificado
- **Plan de contingencia:** conjunto de acciones inmediatas, recursos, responsables y tiempos establecidos para hacer frente a la materialización del riesgo y garantizar la continuidad del servicio
- **Probabilidad:** medida para estimar cuantitativa y cualitativamente la posibilidad de ocurrencia del riesgo.

- **Procedimiento:** conjunto de especificaciones, relaciones, responsabilidades, controles y ordenamiento de las actividades y tareas requeridas para cumplir con el proceso.
- **Proceso:** conjunto de entradas tangibles o intangibles, suministradas por un proveedor, a estas entradas se les asigna recursos y se aplican controles, obteniendo salidas tangibles o intangibles, destinadas a un usuario, generando un impacto en estos. Se clasifican en estratégicos, misionales, de apoyo y de evaluación.
- **Riesgo:** eventualidad que tendrá un impacto negativo sobre los objetivos institucionales o del proceso.

RESPONSABLES

- Subdirección Administrativa y Financiera
- Subdirección Tecnocientífica
- Gestión de las Tecnologías
- Control Interno
- Comunicaciones

MARCO NORMATIVO

- 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

POLÍTICA DE ADMINISTRACIÓN DEL RIESGO

Todo el personal que labora en la ESE Manuel Castro Tovar se comprometen a:

1. Conocer y cumplir las normas de su proceso y procesos transversales relacionadas con la administración de los riesgos.
2. Reportar eventos de riesgo que se materialicen, utilizando los procedimientos e instrumentos establecidos para el efecto.

3. Presentar propuestas de mejora continua de acuerdo a la experiencia en su proceso, en las reuniones pautadas por el líder de proceso.

La Gerencia y las subdirecciones Administrativa y Técnico-Científica se comprometen a gestionar recursos Humanos, presupuestales y tecnológicos necesarios para cumplir con los objetivos trazados en este documento.

DESCRIPCIÓN DEL PLAN

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.

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.

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 otros.

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.

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, Perdidas económicas, Perjuicio de la imagen, Sanciones legales, reproceso, Demoras, Insatisfacción, entre otras.

Barreras de Seguridad Existentes:

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:

PROBABILIDAD		
Remota	1	La probabilidad de ocurrencia es muy baja, casi nula
Poco Probable	2	Puede ocurrir bajo circunstancias excepcionales
Probable	3	Puede ocurrir con cierta frecuencia
Ocasional	4	Ocurre algunas veces
Frecuente	5	La ocurrencia se da de manera comun en circunstancias actuales

IMPACTO		
Muy bajo	1	Los efectos de materializacion del riesgo no son significativos
Bajo	2	Los efectos de materializacion del riesgo son poco significativos
Moderado	3	Los efectos de materializacion del riesgo pueden significar aspectos moderados
Alto	4	Los efectos de materializacion del riesgo son significativos e importantes
Muy Alto	5	Los efectos son catastroficos, como muerte, lesiones incapacitantes o liquidacion de la empresa

PROBABILIDAD						
	5	5	10	15	20	25
	4	4	8	12	16	20
	3	3	6	9	12	15
	2	2	4	6	8	10
	1	1	2	3	4	5
		1	2	3	4	5
		IMPACTO				

NIVEL DE RIESGO	MEDIDAS DE RESPUESTA
BAJA	ASUMIR EL RIESGO Y CONTINUAR MONITORIZANDOLO
ACEPTABLE	REDUCIR EL RIESGO PARA LLEVARLO A ZONA BAJA
ALTA	EVITAR-COMPARTIR-TRANSFERIR POR MEDIO DE UN PLAN DOCUMENTADO
INACEPTABLE	EVITAR-COMPARTIR-TRANSFERIR POR MEDIO DE UN PLAN DOCUMENTADO

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.

IDENTIFICACIÓN DEL RIESGO	FECHA DE IDENTIFICACIÓN	ANÁLISIS DEL RIESGO			VALORACIÓN INICIAL DEL RIESGO			TRATAMIENTO Y SEGUIMIENTO DEL RIESGO						
		CAUSAS	CONSECUENCIAS	BARRERAS DE SEGURIDAD EXISTENTES	VALOR DE PROBABILIDAD	VALOR DE IMPACTO	NIVEL DEL RIESGO	BARRERAS A IMPLEMENTAR	RESPONSBLE	INDICADOR	LINEA BASE	META	RESULTADOS DE EFECTIVIDAD	VALORACIÓN DEL RIESGO DESPUES DE LOS CONTROLES (Control Interno)
Perdida o adulteración de información	31/01/2019	Virus, Daños de Hardware, Uso Indebido del Sistema de Información	Sanciones legales, perdida de Información, Perdidas Económicas	Plan de Backups, Políticas de Seguridad y Privacidad de la Información, Antivirus, UPS.	2	4	8	Seguimiento y Análisis de resultados del Plan de Riesgos de Seguridad y Privacidad de la Información	Gestión de las Tecnologías	Calificación de autodiagnóstico de MIPG superior al 60%	10%	60%		
Uso indebido de la información	31/01/2019	Desconocimiento de la política de Seguridad y Privacidad de la Información	Perdidas económicas, sanciones legales, Daños a Terceros	Política de Seguridad y Privacidad de la Información	3	5	15	Auditoría de los Sistemas de Información, Seguimiento al Plan de TRSPI	Gestión de las Tecnologías, Control Interno, Subdirección Administrativa, Subdirección Técnico-Científica	Calificación de autodiagnóstico de MIPG superior al 60%	10%	60%		

CONTROL DE CAMBIOS

VERSIÓN	APROBACIÓN	DESCRIPCIÓN DEL CAMBIO
01		Versión inicial implementación SGC