HOSPITAL CIVIL DE IPIALES
EMPRESA SOCIAL DEL ESTADO

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

CODIGO: MP - 0446
VERSION: 4
VIGENCIA: 31/01/2025
REVISIÓN: 31/01/2025

ELABORÓ	REVISÓ	APROBÓ
ROBINSON PROAÑO QUISTIAL LIDER GERENCIA DE LA INFORMACION	GABRIELA CHAMORRO HUERTAS P.U GESTION DE CALIDAD	JESSIKA BONILLA SANTIUSTY EN PLANEACION
FECHA 31 – ENERO - 2025	**FECHA** 31 – ENERO - 2025	**FECHA** 31 – ENERO - 2025

2025

Contenido

1. INTRODUCCIÓN 3
2. OBJETIVOS 3
OBJETIVO GENERAL 3
OBJETIVOS ESPECÍFICOS 3
3. ALCANCE 4
4. RESPONSABLES 4
5. MARCO CONCEPTUAL 5
6. MARCO NORMATIVO 6
7. DESCRIPCIÓN DEL PLAN 8
8. BIBLIOGRAFÍA 15

1. INTRODUCCIÓN

El Hospital Civil de Ipiales E.S.E., en busca de la mejora continua, implementa un método lógico y sistemático que permita identificar, analizar, evaluar, tratar, monitorear y comunicar los riesgos asociados al manejo de la información institucional; para lograr que estos riegos no afecten de una manera relevante y significativa al normal funcionamiento de los procesos y la atención de los usuarios.

La institución en su quehacer diario utiliza tecnologías de información, para la captura, procesamiento y reporte de información tanto internamente como externamente para comunicarse con los diferentes actores del sistema de salud; lo cual implica que la institución sea vulnerable a posibles ataques de información al utilizar tecnologías como internet o debido a la mala manipulación de la información por parte de los usuarios, situación que podría acarrear problemas económicos, legales, y administrativos. Por lo cual este documento busca establecer una línea de trabajo que permita a la entidad manejar y mitigar los riesgos que puedan ocasionar perjuicios y mantener la información segura y oportuna.

2. OBJETIVOS

OBJETIVO GENERAL

Desarrollar un Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información que permita el control y minimización de los de los riesgos y de esta forma proteger de mejor manera la privacidad, confidencialidad, disponibilidad y continuidad de la información de la institución y de sus clientes tanto internos como externos.

OBJETIVOS ESPECÍFICOS

- Lograr un diagnóstico real de la situación actual de la institución en materia de riesgos de seguridad y privacidad de la Información

- Aplicar las metodologías, mejores prácticas y recomendaciones dadas por la función pública y Ministerio de la tecnología de la información para el Tratamiento de Riesgos de Seguridad y Privacidad de la Información

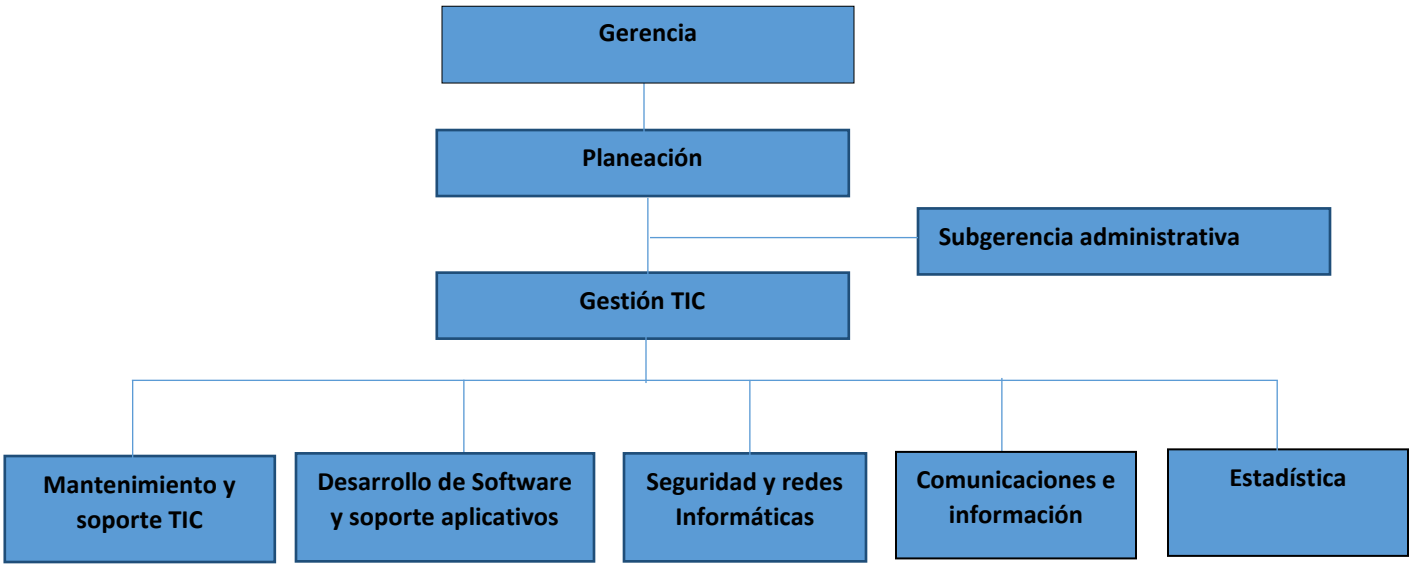
- Optimización de los recursos de la institución en la aplicación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información

3. ALCANCE

El plan de Riesgos de Seguridad y Privacidad aplica a todos los procesos de la institución los cuales manejan, procesan o interactúen con información institucional.

4. RESPONSABLES

La estructura organizacional del proceso de Gestión TIC del Hospital civil de Ipiales es de la siguiente manera:



- Gerente
- Jefe de planeación
- Subgerente Administrativo
- Líder del proceso de Gestión Tic
- Profesional del área de estadística
- Profesional del área de comunicaciones
- Técnico en mantenimiento de computadores
- Auxiliares en mantenimiento de computadores
- Técnicos en desarrollo de software.
- Auxiliares de información

5. MARCO CONCEPTUAL

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.

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

Ciberseguridad: Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética.

Ciberespacio: Ámbito o espacio hipotético o imaginario de quienes se encuentran inmersos en la civilización electrónica, la informática y la cibernética. (CONPES 3701, Tomado de la Academia de la lengua española). 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.

Declaración de aplicabilidad: Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001. (ISO/IEC 27000).

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).

Plan de continuidad del negocio: Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro.
(ISO/IEC 27000).

Plan de tratamiento de riesgos: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

Seguridad de la información: Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

Sistema de Gestión de Seguridad de la Información SGSI: Conjunto de elementos interrelacionados interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).

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.

6. MARCO NORMATIVO

- Anexo 1 - Resolución 3564 de 2015 - Reglamenta aspectos relacionados con la Ley de Transparencia y Acceso a la Información Pública
- Decreto Reglamentario Único 1081 de 2015 - Reglamento sobre la gestión de la información pública
- Título 9 - Decreto 1078 de 2015 - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones
- Ley 1712 de 2014 - Ley de Transparencia y acceso a la información pública
- Ley 57 de 1985 -Publicidad de los actos y documentos oficiales
- Ley 594 de 2000 - Ley General de Archivos

- Título 9 - Decreto 1078 de 2015 - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones

- Título 9 - Decreto 1078 de 2015 - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones

- Ley Estatutaria 1757 de 2015 - Promoción y protección del derecho a la participación democrática

- Título 9 - Decreto 1078 de 2015 - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones

- Ley estatutaria 1618 de 2013: Ejercicio pleno de las personas con discapacidad

- Título 9 - Decreto 1078 de 2015 - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones

- Ley 1437 de 2011: Código de Procedimiento Administrativo y de lo Contencioso Administrativo

- Acuerdo 03 de 2015 del Archivo General de la Nación Lineamientos generales sobre la gestión de documentos electrónicos

- Título 9 - Decreto 1078 de 2015 - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones

- Acuerdo 03 de 2015 del Archivo General de la Nación Lineamientos generales sobre la gestión de documentos electrónicos

- Decreto 019 de 2012 - Suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública
- Decreto 2364 de 2012 - Firma electrónica

- Ley 962 de 2005 - Racionalización de trámites y procedimientos administrativos procedimientos administrativos

- Decreto 1747 de 2000 - Entidades de certificación, los certificados y las firmas digitales

- Ley 527 de 1999 - Ley de Comercio Electrónico

- Decreto Ley 2150 de 1995 - Suprimen y reforman regulaciones, procedimientos o trámites innecesarios existentes en la Administración Pública

- Título 9 - Decreto 1078 de 2015 - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones

- 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

7. DESCRIPCIÓN DEL PLAN

Identificación del riesgo:

El propósito de la identificación del riesgo es determinar que eventos pueden suceder y que cause una perdida potencial de información, y llegar a comprender el cómo, donde, y por qué podría realizarse esa 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.

CL: Clínico: Relacionados a condiciones patológicas de pacientes atendidos en el HCI, considerar la aplicación de la metodología AMFE según lo definido en el MP-0266 MANUAL DE GESTION INTEGRAL DEL RIESGO.

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, pérdidas 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.

	Impacto	Causa Inmediata	Causa Raíz	Descripción del Riesgo	Clasificación del Riesgo	Frecuencia con la cual se realiza la actividad	Probabilidad Inherente
GESTION TIC	Económico y Reputacional	Daño en hardware critico de la institución	Falta de implementación de controles físicos y técnicos al hardware critico de la institución	Perdida de continuidad del negocio debido a que los procesos de consulta, registros y procesamiento de información clínica y administrativa ubicada en los sistemas de información queda deshabilitado.	Fallas Tecnológicas	1	**Muy Baja**
GESTION TIC	Económico y Reputacional	Favorecimiento de un tercero por la manipulación de los activos de la información	Falta de implementación de controles administrativos, físicos y técnicos sobre los activos de la información.	Alteración y/o manipulación indebida de la información asistencial y administrativa contenida en los sistemas de información institucionales o activos de la información priorizados para el favorecimiento a terceros.	Fraude Interno	2	**Muy Baja**

EJE ESTRATEGICO PLAN DE DESARROLLO	OBJETIVO ESTRATEGICO	FUENTE DE COMPROMISOS	DIMENSIONES DEL MIPG	POLITICA DE GESTION Y DESEMPEÑO INSTITUCIONAL	ALINEACION CON OTROS PLANES	PROCESO ASOCIADO	META	ACTIVIDADES PLANEADAS	
Realizar el diagnóstico de riesgos de seguridad y privacidad de la información para la vigencia, constituyéndola a través de la herramienta de autodiagnóstico del modelo de seguridad y privacidad de la información (MSPI)	**Incrementar los niveles de satisfacción del usuario y su familia mediante la prestación de servicios de salud con calidad, oportunidad, seguridad y humanización.**	**Plan de desarrollo institucional 2024-2028**	**Información con valores para resultados**	**Gobierno y seguridad digital**	**Acreditación, PETI, Plan de seguridad de la información**	**GESTION TIC**	**Lograr el 100% en la valoración, identificación y actualización de los riesgos de información.**	**P**	Cronograma para la actualización de matriz de riesgos
								H	Ejecutar cronograma de actualización de inventarios de activos de la información
								H	Identificación de riesgos
								H	Elaboración de la matriz de riesgos
								V	Revisión de cumplimiento de actividades propuestas
								A	Toma de decisiones de acuerdo a los hallazgos encontrados
Realizar el diagnóstico de riesgos de seguridad y privacidad de la información para la vigencia, constituyéndola a través de la herramienta de autodiagnóstico	**Incrementar los niveles de satisfacción del usuario y su familia mediante la prestación de servicios de salud con calidad,**	**Plan de desarrollo institucional 2024-2028**	**Información con valores para resultados**	**Gobierno y seguridad digital**	**Acreditación, PETI, Plan de seguridad de la información**	**GESTION TIC**	**Lograr el 100% en la implementación del plan de tratamiento de riesgos de la información.**	**P**	Levantar cronograma de trabajo para el plan de tratamiento de riesgos de la información
								H	Ejecutar cronograma planteado para el plan de tratamiento de riesgos de la información.
								V	Verificar seguimiento trimestral del plan de trabajo propuesto.

del modelo de seguridad y privacidad de la información (MSPI)	**oportunidad, seguridad y humanización.**							**A**	Toma de decisiones de acuerdo a los hallazgos encontrados.
Realizar el diagnóstico de riesgos de seguridad y privacidad de la información para la vigencia, constituyéndola a través de la herramienta de autodiagnóstico del modelo de seguridad y privacidad de la información (MSPI)	**Incrementar los niveles de satisfacción del usuario y su familia mediante la prestación de servicios de salud con calidad, oportunidad, seguridad y humanización.**	**Plan de desarrollo institucional 2024-2028**	**Información con valores para resultados**	**Gobierno y seguridad digital**	**Acreditación, PETI, Plan de seguridad de la información**	**GESTION TIC**	**Realizar pruebas de penetración (Pentesting) y simulacros de ataques para evaluar la resistencia del sistema ante posibles amenazas.**	**P**	Levantar cronograma de trabajo para el plan de tratamiento de riesgos de la información
								H	Ejecutar cronograma planteado para el plan de tratamiento de riesgos de la información.
								V	Verificar seguimiento trimestral del plan de trabajo propuesto.
								A	Toma de decisiones de acuerdo a los hallazgos encontrados

8. BIBLIOGRAFÍA

Mintic - http://www.mintic.gov.co/

http://estrategia.gobiernoenlinea.gov.co/623/articles-8258_recurso_1.pdf

Mintic - http://www.mintic.gov.co/

http://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html

Mintic - http://www.mintic.gov.co/

https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf