HOSPITAL CIVIL DE IPIALES
EMPRESA SOCIAL DEL ESTADO

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

CODIGO: MN - 0446
VERSION: 5
VIGENCIA: 30/01/2026
REVISIÓN: 30/01/2026

ELABORÓ	REVISÓ	APROBÓ
Robinson Proaño Quistial Líder gerencia de la información	Gabriela Chamorro Huertas Asesora de planeación	Eduardo Narváez Cujar Gerente
FECHA 30 – Enero - 2026	**FECHA** 30 – Enero - 2026	**FECHA** 30 – Enero - 2026

Tabla de contenido

1. INTRODUCCIÓN.

El Hospital Civil de Ipiales E.S.E., en cumplimiento de su misión institucional y el compromiso con la mejora continua, establece el presente Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información. Este documento define un método lógico y sistemático para identificar, analizar, evaluar y tratar los riesgos asociados a los activos de información, garantizando que las amenazas detectadas no afecten de manera significativa la prestación de los servicios de salud ni el funcionamiento administrativo.

En un entorno de transformación digital, la institución utiliza tecnologías de la información para la captura, procesamiento y reporte de datos clínicos y administrativos. Esta dependencia tecnológica genera vulnerabilidades ante amenazas cibernéticas o una inadecuada manipulación de los datos. Por tanto, este plan se alinea con los estándares de la norma ISO/IEC 27001:2022 y los lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones (Min TIC), asegurando la preservación de la Confidencialidad, Integridad y Disponibilidad de la información.

Asimismo, este plan integra la gestión de la Privacidad y Protección de Datos Personales, dando cumplimiento a la Ley Estatutaria 1581 de 2012 y la Ley 1712 de 2014. Con su implementación, el Hospital busca mitigar riesgos legales, económicos y reputacionales, fortaleciendo la confianza de los pacientes y asegurando la resiliencia institucional frente a incidentes de seguridad digital.

2. OBJETIVOS.

2.1 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.

2.2 OBJETIVOS ESPECÍFICOS

- Realizar un diagnóstico y actualización anual de la situación de riesgo de la institución, utilizando la herramienta de autodiagnóstico del Modelo de Seguridad y Privacidad de la Información (MSPI) de MinTIC para identificar brechas técnicas y administrativas.
- Implementar y monitorear los controles de seguridad física, lógica y organizacional definidos en el Anexo A de la norma ISO/IEC 27001:2022, con el fin de mitigar los riesgos identificados en los activos de información críticos del hospital.
- Fortalecer la cultura de seguridad y privacidad en todos los colaboradores y procesos de la institución, mediante programas de capacitación y sensibilización

sobre el manejo adecuado de datos personales y la prevención de delitos informáticos.

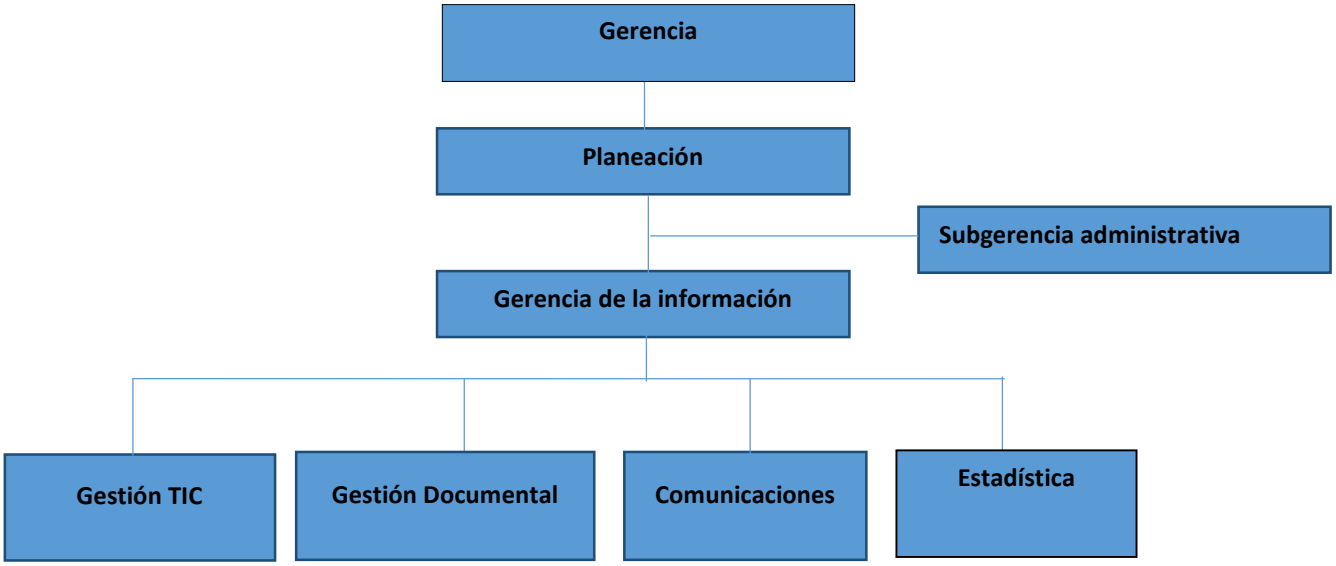
- Evaluar la eficacia del Plan de Tratamiento de Riesgos a través de indicadores de gestión y resultados, permitiendo la toma de decisiones basada en datos y el cumplimiento de las metas reportadas en el Formulario Único de Reporte de Avance a la Gestión (FURAG).
- Garantizar la resiliencia institucional ante incidentes de seguridad digital, mediante la ejecución de pruebas de vulnerabilidad (pentesting) y el fortalecimiento de los planes de continuidad del negocio y recuperación de desastres.

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 Gerencia de la información del Hospital civil de Ipiales se presenta a continuación:



- Gerente
- Jefe de planeación
- Subgerente Administrativo
- Líder del proceso de Gerencia de la información
- Profesional del área de estadística
- Profesional del área de comunicaciones
- Profesional del área de Gestión Documental.
- Ingeniero de seguridad de la información
- Ingeniero de soporte de infraestructura TI

- Técnicos en mantenimiento de computadores
- Ingenieros de desarrollo de software.
- Comité de Seguridad Digital: En cual se toman todas las directrices y decisiones con los informes.

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 27001:2022).

Amenazas: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27001:2022).

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 27001:2022).

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 27001:2022).

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 27001:2022).

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 27001:2022).

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 27001:2022).

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 27001:2022).

Seguridad de la información: Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27001:2022).

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 27001:2022).

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 27001:2022).

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27001:2022).

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

- El Decreto 338 de 2022, establece los lineamientos para fortalecer la gobernanza de la seguridad digital en Colombia.
- El Decreto 1078 de 2015, modelo y las instancias de gobernanza, así como la gestión de riesgos y la identificación de infraestructuras críticas cibernéticas.

7. ALINEACIÓN CON LA PLATAFORMA ESTRATÉGICA INSTITUCIONAL.

La gestión de riesgos de seguridad y privacidad de la información en el Hospital Civil de Ipiales E.S.E. se articula de manera transversal con el Plan de Desarrollo Institucional 2024-2028. El presente plan actúa como un mecanismo de control preventivo para asegurar que los objetivos estratégicos no se vean comprometidos por incidentes que afecten la integridad o disponibilidad de la información asistencial y administrativa.

Esta alineación se materializa a través de los siguientes ejes:

Misión y Visión Institucional: El tratamiento de los riesgos garantiza la confianza y seguridad en la prestación de servicios de salud, protegiendo el activo más valioso de nuestros pacientes: su información clínica.

Objetivo Estratégico de Calidad y Humanización: Al mitigar riesgos de acceso indebido o pérdida de datos, se asegura una atención oportuna y segura, cumpliendo con la meta institucional de incrementar los niveles de satisfacción del usuario y su familia.

Dimensión 4 del MIPG (Gestión con Valores para Resultados): Este plan constituye la base operativa de la Política de Gobierno Digital y Seguridad Digital, integrando el tratamiento de riesgos con la planeación institucional para optimizar el uso de los recursos TIC.

Vinculación con proyectos PETI: Cada acción de tratamiento definida en este documento se enlaza directamente con los proyectos del Plan Estratégico de Tecnologías de la Información (PETI), tales como el fortalecimiento de la infraestructura tecnológica (P8) y la evolución del Sistema de Información Hospitalario (P1 - HIS).

De esta forma, el Plan de Tratamiento de Riesgos deja de ser un requisito técnico para convertirse en un componente esencial de la gobernanza institucional, asegurando que la tecnología sea un habilitador seguro para alcanzar la visión del Hospital hacia el 2028.

Objetivo Estratégico (PDI 2024-2028)	**Riesgo Institucional que lo Amenaza**	**Impacto en la Estrategia**	**Control/Tratamiento Clave**
Incrementar los niveles de satisfacción del usuario y su familia.	**Tratamiento indebido de datos personales de salud.**	Pérdida de confianza del paciente y posibles sanciones legales de la SIC por vulnerar el Habeas Data.	**Control 5.34 (ISO 27001):** Jornadas de socialización de la política de privacidad y protección de datos personales.

Objetivo Estratégico (PDI 2024-2028)	Riesgo Institucional que lo Amenaza	Impacto en la Estrategia	Control/Tratamiento Clave
Garantizar la seguridad y humanización en la prestación de servicios.	**Indisponibilidad de sistemas asistenciales (HIS).**	Retraso en la atención médica crítica por falta de acceso a la historia clínica, afectando la seguridad del paciente.	**Control 5.30 y 8.13:** Simulacros de restauración de backups y plan de continuidad ante desastres.
Fortalecer la gestión administrativa y financiera con transparencia.	**Fraude interno por manipulación de información.**	Alteración de registros administrativos para favorecer a terceros, afectando la transparencia institucional.	**Control 8.15 y 8.18:** Revisión trimestral de logs de auditoría y gestión estricta de privilegios de acceso.

8. 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 de acuerdo a la normatividad **ISO/IEC 27001:2022**, 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.

Riesgo Institucional Identificado	**Proyecto PETIC Relacionado**	**Actividad Planeada (Tratamiento)**	**Control ISO/IEC 27001:2022**	**Indicador de Seguimiento (Eficacia)**
Tratamiento indebido de datos personales de salud	P4 – Seguridad de la Información	Actualizar los avisos de privacidad y realizar jornadas de socialización de la política de tratamiento de datos personales.	**5.34** Privacidad y protección de PII.	% de personal asistencial capacitado en Ley 1581 de 2012.
Pérdida, acceso indebido o daño de información	P4 – Seguridad de la Información	Ejecutar cronograma de actualización de inventarios de activos de información y parches de seguridad.	**8.12** Gestión de vulnerabilidades técnicas.	(Vulnerabilidades remediadas / Vulnerabilidades detectadas) x 100.
Fraude interno por uso indebido de información	P4 – Seguridad de la Información	Realizar revisiones trimestrales de los logs de auditoría en los sistemas de información institucionales.	**8.15** Registro de eventos y **8.18** Privilegios de acceso.	Número de auditorías de acceso ejecutadas según cronograma.

Riesgo Institucional Identificado	Proyecto PETIC Relacionado	Actividad Planeada (Tratamiento)	Control ISO/IEC 27001:2022	Indicador de Seguimiento (Eficacia)
Daño de hardware crítico	P8 – Infraestructura tecnológica	Ejecutar el plan de mantenimiento preventivo y asegurar la redundancia de equipos críticos.	**8.14** Redundancia de las instalaciones.	% de disponibilidad de los servidores críticos del Hospital.
Indisponibilidad de sistemas asistenciales	P1 – HIS / P8 – Infraestructura	Realizar simulacros de restauración de backups y actualizar planes de continuidad.	**8.13** Respaldo de información y **5.30** Continuidad.	Tiempo de recuperación (RTO) logrado en simulacros vs. meta.
Acceso indebido a historia clínica física	P4 – Seguridad / P1 – HIS	Fortalecer perímetros de seguridad física en archivo y avanzar en la digitalización de expedientes.	**7.1** Perímetros de seguridad física.	% de historias clínicas digitalizadas con firma electrónica.

Tabla de tratamiento de riesgos de Gerencia de la información.

9. CONCLUSIÓN TÉCNICA.

La implementación del presente Plan de Tratamiento de Riesgos representa el compromiso del Hospital Civil de Ipiales E.S.E. con la protección de sus activos de información y la privacidad de sus usuarios. Al alinear las actividades de tratamiento con los proyectos estratégicos del PETIC y los controles de la norma ISO/IEC 27001:2022, la institución no solo mitiga vulnerabilidades técnicas y operativas, sino que fortalece su resiliencia ante incidentes de seguridad digital.

El cumplimiento de este plan, monitoreado a través de indicadores de eficacia, garantiza que la gestión del riesgo sea un proceso dinámico y sistemático que soporte la toma de decisiones basada en datos. Este enfoque asegura la continuidad de los servicios asistenciales, la integridad de las historias clínicas y el cumplimiento riguroso del marco legal colombiano, contribuyendo directamente a la excelencia en la prestación de servicios de salud y al éxito en la medición del Modelo Integrado de Planeación y Gestión (MIPG/FURAG).

10. 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