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

EMPRESA SOCIAL DEL ESTADO
HOSPITAL LA MARÍA
MEDELLÍN
Trabajamos con amor por la vida desde 1923

MEDELLÍN
2025

Calle 92 EE No 67-61 PBX 447192 NIT 890.905.177-9 Medellin, Colombia
gerencia@lamaria.gov.co/www.lamaria.gov.co

CONTENIDO

Calle 92 EE No 67-61 PBX 447192 NIT 890.905.177-9 Medellin, Colombia
gerencia@lamaria.gov.co/www.lamaria.gov.co

1. INTRODUCCIÓN

El Hospital La María reconoce la importancia de la información en sus procesos misionales y administrativos. El tratamiento adecuado de los riesgos relacionados con la seguridad y privacidad de la información digital es esencial para garantizar la confidencialidad, integridad y disponibilidad de los activos informacionales. Este plan se formula en cumplimiento de las directrices del MinTIC y la normativa vigente, y contempla además la obligación de reporte y atención de incidentes de seguridad digital ante las entidades competentes del Estado.

2. OBJETIVOS

2.1. Objetivo General

Establecer políticas, procedimientos y medidas de seguridad para garantizar la protección de la información y fomentar una cultura de seguridad institucional.

2.2. Objetivo Específicos

A. Identificar y evaluar los riesgos que afectan la seguridad de la información.

B. Definir roles y responsabilidades frente al tratamiento de riesgos.

C. Implementar controles técnicos y organizativos adecuados.

D. Fomentar la cultura de seguridad mediante capacitaciones.

E. Establecer procedimientos para el manejo y reporte de incidentes.

F. Determinar ciclos de auditoría para evaluar la efectividad del sistema.

3. MARCO NORMATIVO

NTC / ISO 27001:2013 Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI).

a. Constitución Política de Colombia: Reconoce el derecho fundamental a la privacidad, el cual incluye la protección de los datos personales.

b. Ley 1581 de 2012: Establece el régimen general de protección de datos personales, y regula el manejo de esta información por parte de personas naturales y jurídicas, de naturaleza pública o privada.

c. Decreto 1377 de 2013: Reglamenta parcialmente la Ley 1581 de 2012, y

establece los requisitos y procedimientos para la protección de datos personales.

d. **Resolución 1995 de 1999**: Establece las normas para el manejo de historias clínicas en Colombia, y regula el acceso a la información médica.

e. **Resolución 1860 de 2018**: Regula el manejo de datos personales en el sector salud, y establece los requisitos para la implementación de medidas de seguridad y privacidad en la información de los pacientes.

f. **Circular 007 de 2022 - MinTIC** (reporte obligatorio de incidentes de seguridad digital en RNIS)

4. ALCANCE

Este plan aplica a todos los procesos, sistemas y personal del Hospital La María, incluyendo contratistas y terceros con acceso a la información institucional.

5. METODOLOGÍA DE GESTIÓN DEL RIESGO

El plan sigue las etapas recomendadas por el MSPI y la ISO 27005:

- Identificación de activos de información
- Análisis y evaluación de amenazas y vulnerabilidades
- Valoración del riesgo
- Determinación del riesgo aceptable
- Plan de tratamiento

6. ACTIVIDADES

6.1 Identificación y Evaluación:

- Reunión con líderes de procesos
- Aplicación de metodología de riesgo digital

6.2 Clasificación de Activos:

- Cada líder de proceso es responsable por la identificación y clasificación de los activos de información bajo su control.
- El Área de Archivo General y Gestión Documental consolida y mantiene actualizado el inventario institucional.

6.3 Evaluación de Amenazas y Vulnerabilidades:

- Análisis de escenarios internos y externos

6.4 Tratamiento del Riesgo:

- Aprobación y aceptación de riesgos
- Definición de controles correctivos y preventivos

6.5 Reporte de Incidentes:

- Todos los incidentes de seguridad digital deberán ser reportados a través del portal oficial del RNIS (https://rnis.gov.co), conforme a la Circular 007 de 2022 del MinTIC.
- El CISO es el encargado de asegurar el reporte oportuno, la clasificación y el seguimiento de cada incidente.

7. SEGUIMIENTO Y CONTROL

El seguimiento y control se realiza mediante la oficina de control interno y el comité institucional de gestión y desempeño.

8. ROLES Y RESPONSABILIDADES

- Alta Gerencia: Aprobación del plan, asignación de recursos y liderazgo institucional del enfoque de seguridad.
- Líderes de proceso: Identificación y clasificación de activos de información, evaluación de riesgos asociados a sus procesos y ejecución de acciones de mitigación.
- Archivo General y Gestión Documental: Consolidación y mantenimiento del inventario institucional de activos de información.
- Oficina de Calidad: Integración del tratamiento de riesgos en la gestión de calidad y evaluación continua de procesos.
- Control Interno: Verificación del cumplimiento del plan, revisión documental y acompañamiento en la mejora continua.
- Área Jurídica: Asesoría normativa en temas relacionados con protección de datos personales y cumplimiento legal.
- Oficina de Planeación: Alineación del plan con la planeación estratégica institucional.

Calle 92 EE No 67-61 PBX 447192 NIT 890.905.177-9 Medellin, Colombia
gerencia@lamaria.gov.co/www.lamaria.gov.co

- CISO / Área TIC: Apoyo técnico en metodologías, herramientas, y acompañamiento en el reporte y gestión de incidentes a través del RNIS.

- Todos los colaboradores: Participación activa en la identificación de riesgos y cumplimiento de las acciones preventivas y correctivas definidas.

9. DICCIONARIO

- Activo de información: es todo aquello se genera en las entidades consideran importante o de alta validez para la misma ya que puede contener importante información como lo puede ser contraseñas, números de cuentas, Historia Clínicas etc.
- Análisis de riesgo: busca establecer la probabilidad de ocurrencia de los riesgos y el impacto de sus consecuencias, calificándolos y evaluándolos con el fin de obtener información para establecer el nivel de riesgo y las acciones que se van a implementar.
- Consecuencias: generalmente se da sobre las personas o los bienes materiales o inmateriales con incidencias importantes tales como; daños físicos, fallecimiento, pérdidas económicas, de información, de bienes, de imagen, de credibilidad y de confianza, interrupción del servicio y daño material.
- Controles correctivos: aquellos que permiten el restablecimiento de la actividad después de ser detectado un evento no deseable; también permiten la modificación de las acciones que propiciaron su ocurrencia.
- Controles preventivos: aquellos que actúan para eliminar las causas del riesgo para prevenir su ocurrencia o materialización.
- Generador de riesgo: origen de donde provienen o surge el riesgo.
- Evaluación del riesgo: proceso usado para determinar las prioridades de gestión del riesgo mediante la comparación de los resultados de la calificación y el grado de exposición al riesgo.
- Factibilidad: presencia de factores internos y externos que pueden propiciar el riesgo, aunque éste no se haya materializado.

Calle 92 EE No 67-61 PBX 447192 NIT 890.905.177-9 Medellin, Colombia
gerencia@lamaria.gov.co/www.lamaria.gov.co

- Gestión del riesgo: cultura, procesos y estructuras que se dirigen hacia la gestión audaz de las oportunidades potenciales y los efectos adversos.
- Identificación del riesgo: permite conocer los eventos potenciales, que están o no bajo control de la entidad que ponen en riesgo el logro de su misión.
- Impacto: grado en que las consecuencias pueden generar pérdidas si se llega a materializar el riesgo.
- Mapa de riesgos institucional: contiene a nivel estratégico los mayores riesgos a los cuales está expuesta la entidad, permitiendo conocer las políticas inmediatas de respuesta ante ellos, la conforman los diferentes tipos de riesgos por proceso y de corrupción
- Objetivo del proceso: conjunto de pasos parcialmente ordenados para alcanzar un objetivo dentro de la organización. La transformación desde un estado hacia otro, por medio de agentes coordinados, con el propósito certero de lograr estos objetivos, son derivados de la responsabilidad del encargado del proceso
- Proceso: un proceso es un conjunto de actividades mutuamente relacionadas o que, al interactuar, transforman elementos de entrada y los convierten en resultados. Se soportan en el modelo de operación por procesos y se nombran conforme a la cadena de valor establecida en la entidad, según su propósito que pueden clasificarse en estratégicos, misionales, y de apoyo
- Riesgo: probabilidad de ocurrencia de un evento que puede entorpecer el normal desarrollo de las funciones de la entidad y le impide el logro de sus objetivos
- 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.
- Seguimiento: verificar y evaluar la elaboración, el seguimiento y el control del mapa de riesgos
- Tratamiento del riesgo: selección e implementación de las opciones apropiadas para ocuparse del riesgo.
- Vulnerabilidad: defecto o debilidad en los procedimientos de seguridad, diseño, implementación o en los controles internos de los procesos y los sistemas que podrían ser explotadas.

	NOMBRE – CARGO	FIRMA	FECHA
PROYECTÓ	Sebastián Muñoz Mejía – jefe de Sistemas	Electrónicamente	12-02-25
APROBÓ	Ramon Antonio Lema Hurtado - subgerente	Electrónicamente	12-02-25

Calle 92 EE No 67-61 PBX 447192 NIT 890.905.177-9 Medellin, Colombia
gerencia@lamaria.gov.co/www.lamaria.gov.co