PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2025

APROBADO POR:

LUDIS ELENA CHAVEZ BARRIOS

GERENTE ESE

PLANES INSTITUCIONALES DEL MIPG Y DEL MODELO DE PRESTACION DE SERVICIOS DE SALUD DE LA ESE.

DEPARTAMENTO DE BOLIVAR

MUNICIPIO DE MARIA LA BAJA

EMPRESA SOCIAL DEL ESTADO

HOSPITAL LOCAL MARIA LA BAJA

ENERO DE 2025

INTRODUCCION

Mediante la definición del Plan de Tratamiento de Riesgos de la **ESE HOSPITAL LOCAL MARIA LA BAJA** busca mitigar los riesgos presentes en el análisis de riesgos (Perdida de la Confidencialidad, Perdida de Integridad y Perdida de

Dirección: calle 20 N° 8-78. María la Baja-Bolívar
NIT. 806.010.788-1
Email: gerencia@hospitalmarialabaja.com
secretaria@hospitalmarialabaja.com
Telefax: (5)6261103

Disponibilidad), en la información digital, evitando aquellas situaciones que impidan el logro Estratégicos de la ESE.

La gestión de los riesgos de seguridad y la privacidad de la información son los procesos de identificación, evaluación, tratamiento, control y seguimiento de los riesgos inherentes a la seguridad y protección de la información. La finalidad del presente documento es la protección de la información, conociendo las fortalezas y debilidades que pudiesen afectar el servicio tanto misional y como de apoyo.

El plan de tratamiento de riesgos de Seguridad y Privacidad de la información, Seguridad Digital en la **ESE HOSPITAL LOCAL MARIA LA BAJA**, se basa en una orientación estratégica que requiere el desarrollo de una cultura de carácter preventivo en la entidad, de manera que, al comprender el concepto de riesgo, así como el contexto, a través de este instrumento se planean las acciones que reduzcan la afectación a la entidad en caso de materialización de estos, adicional se busca desarrollar estrategias para la identificación, análisis, tratamiento, evaluación y monitoreo de dichos riesgos con mayor objetividad, dando a conocer aquellas situaciones que pueden comprometer el cumplimiento de los objetivos trazados en el mundo en el entorno Digital.

Las anteriores medidas se definen teniendo en cuenta la información del análisis de riesgos, sobre la plataforma informática y las necesidades del Proceso de Gestión de la Infraestructura de TIC de la ESE, en cuanto a la seguridad de la información y proporciona las herramientas necesarias para definir cada una de las características de las medidas y la definición de los pasos a seguir para su ejecución.

Lo anterior dando cumplimiento a la normativa establecida por el estado colombiano, CONPES 3854 de 2016, Modelo de Seguridad y Privacidad de MINTIC y lo establecido en el decreto 1008 de 14 de junio 2018, adoptando las buenas prácticas y los lineamientos del estándar ISO 27001:2013, alineado con ISO 31000:2018 y la guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital - Versión 4

Dirección: calle 20 N° 8-78. María la Baja-Bolívar
NIT. 806.010.788-1
Email: gerencia@hospitalmarialabaja.com
secretaria@hospitalmarialabaja.com
Telefax: (5)6261103

emitida por el Departamento Administrativo de la Funciona Pública y aquellas que La ESE defina.

OBJETIVOS

GENERAL

Establecer los conceptos básicos y metodológicos que permitan tratar de manera integral los riesgos de seguridad digital a los que pueda estar expuesta la institución, para proteger, asegurar y salvaguardar la confidencialidad, integridad y disponibilidad de los activos de información teniendo en cuenta los procesos, la operación, los objetivos de negocio y los requisitos legales vigentes en la entidad.

ESPECIFICOS

- Identificar, valorar, tratar y monitorear de manera efectiva los riesgos que puedan afectar positiva o negativamente la Seguridad y la Privacidad de la información.
- Realizar la gestión y tratamiento de los riesgos identificados y que impacten la Seguridad y la Privacidad de la información.
- Controlar y minimizar los riesgos asociados a los procesos tecnológicos existentes, en la **ESE HOSPITAL LOCAL MARIA LA BAJA**, con el fin de salvaguardar los activos de información, el manejo de medios, control de acceso y gestión de usuarios.
- Cumplir con los requisitos legales y reglamentarios pertinentes a la legislación colombiana en materia de seguridad de la información.
- Fortalecer y apropiar conocimiento referente a la gestión de riesgos Seguridad y Privacidad de la información, Seguridad Digital.

Dirección: calle 20 N° 8-78. María la Baja-Bolívar
NIT. 806.010.788-1
Email: gerencia@hospitalmarialabaja.com
secretaria@hospitalmarialabaja.com
Telefax: (5)6261103

ALCANCE

Con el propósito de realizar una eficiente gestión de riesgos de Seguridad Digital en La **ESE HOSPITAL LOCAL MARIA LA BAJA**, esta actividad se debe realizar integrando los procesos de la entidad con este plan, mediante el uso de buenas prácticas y lineamientos nacionales, y locales, con el propósito que ello contribuya a la toma de decisiones y prevenir incidentes que puedan afectar el logro de los objetivos. A partir de lo anterior se definen los lineamientos mediante una guía de para la gestión de riesgos de Seguridad Digital, para el tratamiento de los riesgos asociados a la información que es soportada por compontes tecnológicos en el entorno digital.

La **ESE- HOSPITAL LOCAL MARIA LA BAJA** propende por la protección de la información física y electrónica que almacena, recolecta, produce y gestiona a través de la implementación de controles físicos y lógicos, gestión de riesgos y la mejora continua, permitiendo incrementar los niveles de confidencialidad, integridad y disponibilidad de la información, apoyándose en los requisitos legales y normativos contribuyendo al cumplimiento misional de la entidad.

ALCANCE:

Con el propósito de realizar una eficiente gestión de riesgos de Seguridad Digital en La **ESE- HOSPITAL LOCAL MARIA LA BAJA**, esta actividad se debe realizar integrando los procesos de la entidad con este plan, mediante el uso de buenas prácticas y lineamientos nacionales, y locales, con el propósito que ello contribuya a la toma de decisiones y prevenir incidentes que puedan afectar el logro de los objetivos. A partir de lo anterior se definen los lineamientos mediante una guía de para la gestión de riesgos de Seguridad Digital, para el tratamiento de los riesgos asociados a la información que es soportada por compontes tecnológicos en el entorno digital.

Dirección: calle 20 N° 8-78. María la Baja-Bolívar
NIT. 806.010.788-1
Email: gerencia@hospitalmarialabaja.com
secretaria@hospitalmarialabaja.com
Telefax: (5)6261103

La **ESE- HOSPITAL LOCAL MARIA LA BAJA** propende por la protección de la información física y electrónica que almacena, recolecta, produce y gestiona a través de la implementación de controles físicos y lógicos, gestión de riesgos y la mejora continua, permitiendo incrementar los niveles de confidencialidad, integridad y disponibilidad de la información, apoyándose en los requisitos legales y normativos contribuyendo al cumplimiento misional de la entidad.

DEFINICIONES:

A continuación, se listan algunos términos y definiciones de términos que se utilizarán durante el desarrollo de la gestión de riesgos de seguridad de la información, en beneficio de unificar criterios dentro de La **ESE- HOSPITAL LOCAL MARIA LA BAJA**

Administración del Riesgo: Conjunto de elementos de control que al interrelacionarse brindan a la entidad la capacidad para emprender las acciones necesarias que le permitan el manejo de los eventos que puedan afectar negativamente el logro de los objetivos institucionales y protegerla de los efectos ocasionados por su ocurrencia.

Activo de Información: En relación con la seguridad de la información, se refiere a cualquier información o elemento de valor para los procesos de la organización.

Análisis de riesgos: Es un método sistemático de recopilación, evaluación, registro y difusión de información necesaria para formular recomendaciones orientadas a la adopción de una posición o medidas en respuesta a un peligro determinado.

Amenaza: Es la causa potencial de una situación de incidente y no deseada por la organización.

Dirección: calle 20 N° 8-78. María la Baja-Bolívar
NIT. 806.010.788-1
Email: gerencia@hospitalmarialabaja.com
secretaria@hospitalmarialabaja.com
Telefax: (5)6261103

Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

Consecuencia: Resultado de un evento que afecta los objetivos.

Criterios del riesgo: Términos de referencia frente a los cuales la importancia de un riesgo se evaluada.

Control: Medida que modifica el riesgo.

Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

Evaluación de riesgos: Proceso de comparación de los resultados del análisis del riesgo con los criterios del riesgo, para determinar si el riesgo, su magnitud o ambos son aceptables o tolerables.

Evento: Un incidente o situación, que ocurre en un lugar particular durante un intervalo de tiempo específico.

Estimación del riesgo: Proceso para asignar valores a la probabilidad y las consecuencias de un riesgo.

Evitación del riesgo: Decisión de no involucrarse en una situación de riesgo o tomar acción para retirarse de dicha situación.

Factores de Riesgo: Situaciones, manifestaciones o características medibles u observables asociadas a un proceso que generan la presencia de riesgo o tienden a aumentar la exposición, pueden ser internos o externos a la entidad.

Dirección: calle 20 N° 8-78. María la Baja-Bolívar
NIT. 806.010.788-1
Email: gerencia@hospitalmarialabaja.com
secretaria@hospitalmarialabaja.com
Telefax: (5)6261103

Gestión del riesgo: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo, se compone de la evaluación y el tratamiento de riesgos.

Identificación del riesgo: Proceso para encontrar, enumerar y caracterizar los elementos del riesgo.

Incidente de seguridad de la información: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información (Confidencialidad, Integridad y Disponibilidad).

Integridad: Propiedad de la información relativa a su exactitud y completitud.

Impacto: Cambio adverso en el nivel de los objetivos del negocio logrados.

Nivel de riesgo: Magnitud de un riesgo o de una combinación de riesgos, expresada en términos de la combinación de las consecuencias y su posibilidad.

Acceso a la información pública: Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4).

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).

Dirección: calle 20 N° 8-78. María la Baja-Bolívar
NIT. 806.010.788-1
Email: gerencia@hospitalmarialabaja.com
secretaria@hospitalmarialabaja.com
Telefax: (5)6261103

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.

Ciberseguridad: Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).

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.

Privacidad: En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente.

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).

Dirección: calle 20 N° 8-78. María la Baja-Bolívar
NIT. 806.010.788-1
Email: gerencia@hospitalmarialabaja.com
secretaria@hospitalmarialabaja.com
Telefax: (5)6261103

Sistemas de Gestión de Seguridad de la Información SGSI: Conjunto de elementos interrelacionados o 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).

MARCO REGULATORIO Y NORMATIVO

La **ESE- HOSPITAL LOCAL MARIA LA BAJA**, como entidad pública, al igual que cualquier organismo del estado, se encuentra cubierta por un marco normativo y regulatorio en todo lo relacionado con la seguridad de la información, como también un marco de referencia de las mejores prácticas para el desarrollo e implementación del Sistema de Gestión de Riesgos de Seguridad y Privacidad de la Información.

La **ESE- HOSPITAL LOCAL MARIA LA BAJA** a través de su Modelo de Seguridad y Privacidad, se compromete a mantener una cultura de la gestión del riesgo digital, con un enfoque basado en los riesgos de seguridad digital en los procesos y proyectos luchando continuamente contra la corrupción, mediante mecanismos, sistemas y controles enfocados a la prevención y detección de hechos asociados a este fenómeno y fortaleciendo las medidas de control y la eficiencia a lo largo del ciclo de vida del proyecto para optimizar de manera continua y oportuna la respuesta a los riesgos además de los de seguridad y privacidad de la Información y Seguridad Digital de manera integral.

La política identifica las opciones para tratar y manejar los riesgos basados en su valoración, permiten tomar decisiones adecuadas y fijar los lineamientos para administración de los mismos; a su vez, transmiten la posición de la dirección y establecen las guías de acción necesarias a todos los colaboradores de la ESE.

Se deben tener en cuenta algunas de las siguientes opciones, las cuales pueden considerarse independientemente, interrelacionadas o en conjunto:

Dirección: calle 20 N° 8-78. María la Baja-Bolívar
NIT. 806.010.788-1
Email: gerencia@hospitalmarialabaja.com
secretaria@hospitalmarialabaja.com
Telefax: (5)6261103

• **Evitar**: es eliminar la probabilidad de ocurrencia o disminuir totalmente el impacto, lo que requiere la eliminación de la actividad o fuente de riesgo del activo, eliminar la exposición y su expresión máxima es dejar una actividad. Por ejemplo, para evitar perdida de archivos se retiran los permisos de acceso.

• **Prevenir:** corresponde al área de planeación, esto es, planear estrategias conducentes a que el evento no ocurra o que disminuya su probabilidad. Un ejemplo de ello son las inspecciones, el mantenimiento preventivo, las políticas de seguridad o las revisiones periódicas a los procesos.

• **Reducir o mitigar:** corresponde a la protección en el momento en que se presenta el riesgo se encuentra en esta categoría los planes de emergencia, planes de continencia equipos de protección personal, ambiental, de acceso, mantener copias de respaldo.

• **Dispersar:** es dividir una actividad en diferentes componentes operativos, de manera que las actividades no se concentren en un mismo sitio o bajo una sola responsabilidad. Este es el caso de los contratos de suministro de partes, la ubicación de nodos, plantas alternas, equipos paralelos, contratar obras por tramos.

• **Compartir:** es involucrar a un tercero para que responda en todo o en parte por el riesgo que genera una actividad. Dentro de los mecanismos de transferencia se encuentran los siguientes:contratos de seguro, transferencia explicita por medio de cláusulas contractuales.

METODOLOGIA DE IMPLEMENTACIÓN

Para llevar a cabo la implementación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, se toma como base la metodología PHVA (Planear, Hacer, Verificar y Actuar) y los lineamientos emitidos por el Ministerio de

Dirección: calle 20 N° 8-78. María la Baja-Bolívar
NIT. 806.010.788-1
Email: gerencia@hospitalmarialabaja.com
secretaria@hospitalmarialabaja.com
Telefax: (5)6261103

Tecnologías de la Información y las Comunicaciones – MinTIC, a través de los decretos emitidos.

De acuerdo con esto, se definen las siguientes fases de implementación del PSPI:

1. Diagnosticar
2. Planear
3. Hacer
4. Verificar
5. Actuar

ACTIVIDADES

• Realizar Diagnóstico
• Realizar la Identificación de los Riesgos con los líderes del Proceso.
• Encuesta con los líderes de cada proceso
• Levantamiento de los riesgos
• Planteamiento del Plan de Tratamiento de Riegos
• Ajustes a Procesos del SGC

FASE	ACTIVIDADES	RESPONSABLE	FECHA INICIO	FECHA FIN
Planeación de la gestion del Riesgo	Revisar y ajustar Metodología para la gestión de Riesgo de Seguridad Digital acorde a las necesidades de la ESE Revisión Guía de	Líder Sistema	Marzo	Abril

Dirección: calle 20 N° 8-78. María la Baja-Bolívar
NIT. 806.010.788-1
Email: gerencia@hospitalmarialabaja.com
secretaria@hospitalmarialabaja.com
Telefax: (5)6261103

	Gestion de Riesgo de seguridad Digital			
Identicación y valoración de Activos	Identicación de Activos de Información. Clasificación de Activos de Información. Valoración de Activos de Información.	Líder Sistemas	Abril	Mayo
Identificación de Amenazas y Vulnerabilidades	Identificación de Amenazas y Vulnerabilidades.	Líder Sistemas	Junio	Junio
Determinación de Riesgos	Determinación del Impacto de las amenazas por activo. Determinación de Probabilidad de Ocurrencia	Líder Sistemas	Julio	Julio
Análisis de Riesgos	Cálculo de Riesgos Identificación de Riesgos superiores	Líder Sistemas	Agosto	Agosto
Gestión de Riesgos	Determinación de Controles Tratamiento de Riesgos Diseño de controles Priorización de Controles	Líder Sistemas	Septiembre	Septiembre
Monitoreo	Medición de la eficacia de los controles	Líder Sistemas y áreas responsables	Noviembre	Noviembre

Dirección: calle 20 N° 8-78. María la Baja-Bolívar
NIT. 806.010.788-1
Email: gerencia@hospitalmarialabaja.com
secretaria@hospitalmarialabaja.com
Telefax: (5)6261103

LINEAMIENTOS ESTRATÉGICOS

La protección debe garantizar en primer lugar la confidencialidad, integridad y disponibilidad de los datos, sin embargo, existen más requisitos como por ejemplo la autenticidad de entre otros.

En la Seguridad de la Información el objetivo de la protección son los datos mismos y tratar de evitar su perdida y modificación no autorizada. La **ESE HOSPITAL LOCAL MARIA LA BAJA** asume el compromiso de implementar el sistema de Gestión del tratamiento de riesgos de la Seguridad y privacidad de la información para proteger los activos de información de los procesos misionales, comprometiéndose a:

• Realizar una gestión integral de riesgos basada en la implementación de controles físicos y digitales orientados a la prevención de incidentes.

• El fomento de la cultura y toma de conciencia entre el personal (funcionarios, contratistas, proveedores y terceros) sobre la importancia de la seguridad de la información.

• Diseñar e implementar una estrategia que permita proteger la información generada, recolectada, procesada y utilizada en el cumplimiento de la misión de la Entidad.

• El proceso de Gestión de Información establecerá los lineamientos para la identificación, clasificación y buen uso de los activos de información físicos y digitales, para su protección.

• Proteger las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.

Dirección: calle 20 N° 8-78. María la Baja-Bolívar
NIT. 806.010.788-1
Email: gerencia@hospitalmarialabaja.com
secretaria@hospitalmarialabaja.com
Telefax: (5)6261103

• Controlar la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.

• Se garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.

LUDIS ELENA CHAVEZ BARRIOS

GERENTE ESE

Dirección: calle 20 N° 8-78. María la Baja-Bolívar
NIT. 806.010.788-1
Email: gerencia@hospitalmarialabaja.com
secretaria@hospitalmarialabaja.com
Telefax: (5)6261103

E.S.E
HOSPITAL LOCAL
MARÍA LA BAJA

¡Tu Salud, Un Compromiso Tuyo y Nuestro!

Dirección: calle 20 N° 8-78. María la Baja-Bolívar
NIT. 806.010.788-1
Email: gerencia@hospitalmarialabaja.com
secretaria@hospitalmarialabaja.com
Telefax: (5)6261103