


PLAN DE TRATAMIENTO DE RIESGOS SEGURIDAD Y PRIVACIDAD DE LA INFORMACION




MADELEINE DIAZ FRANCO
GERENTE ENCARGADA



	VERSION:	03
	FECHA DE ACTUALIZACION:	30-ENE-2025
PLAN DE TRATAMIENTO DE RIESGOS SEGURIDAD Y PRIVACIDAD DE LA INFORMACION	CÓDIGO:	HNSC-GG-M-012
	PAGINA	Página 1 de 24

Contenido


INTRODUCCIÓN	3
OBJETIVOS	4
OBJETIVO GENERAL	4
OBJETIVOS ESPECÍFICOS	4
ALCANCE	5
MARCO LEGAL	6
DEFINICIONES	7
DIRECCIONAMIENTO ESTRATEGICO E.S.E. HOSPITAL NUESTRA SEÑORA DEL CARMEN DE GUAMAL, MAGDALENA	9
IDENTIFICACION GENERAL	9
MISIÓN	9
VISIÓN	10
ROL DE LA E.S.E DENTRO DE LA RED DEPARTAMENTAL	10
PRESTACION DE LOS SERVICIOS	11
VALORES INSTITUCIONALES	11
PRINCIPIOS INSTITUCIONALES	13
MAPA DE PROCESOS	15
ORGANIGRAMA	16
OFERTA DE SERVICIOS DE LA E.S.E. HOSPITAL NUESTRA SEÑORA DEL CARMEN DE GUAMAL – MAGDALENA	17
PORTAFOLIO DE SERVICIOS	17
DESARROLLO DEL TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	18
VALORACIÓN DEL RIESGO	19
IDENTIFICACIÓN DEL RIESGO	19
IDENTIFICACIÓN DE LOS ACTIVOS	19
IDENTIFICACIÓN DE LAS AMENAZAS	19
IDENTIFICACIÓN DE CONTROLES EXISTENTES	20
IDENTIFICACIÓN DE LAS VULNERABILIDADES	20

	VERSION:	03
	FECHA DE ACTUALIZACION:	30-ENE-2025
PLAN DE TRATAMIENTO DE RIESGOS SEGURIDAD Y PRIVACIDAD DE LA INFORMACION	CÓDIGO:	HNSC-GG-M-012
	PAGINA	Página 2 de 24

IDENTIFICACION DEL RIESGO 21

CRONOGRAMA 22

BIBLIOGRAFÍA..... 24

	VERSION:	03
	FECHA DE ACTUALIZACION:	30-ENE-2025
PLAN DE TRATAMIENTO DE RIESGOS SEGURIDAD Y PRIVACIDAD DE LA INFORMACION	CÓDIGO:	HNSC-GG-M-012
	PAGINA	Página 3 de 24

INTRODUCCIÓN


En la actualidad, se vuelve indispensable gestionar los riesgos de todo tipo en las organizaciones, y la Seguridad de la Información no es una excepción. La política de Gobierno Digital establece la necesidad de desarrollar e implementar una Metodología de Gestión de Riesgos, que sirve como base para la elaboración de este documento.

Es importante destacar que la información que forma parte de una entidad pública es vital para su correcto funcionamiento dentro del marco de la política pública y su interacción con los ciudadanos. No importa el tipo de información que se maneje en la entidad; esta se convierte en un elemento esencial para el cumplimiento de sus objetivos. Por ello, proteger toda clase de información de posibles alteraciones, usos indebidos, pérdidas, entre otros eventos, es fundamental para garantizar el normal desarrollo de las actividades de esta entidad hospitalaria.

A través de la definición del Plan de Tratamiento de Riesgos, la E.S.E. Hospital Nuestra Señora del Carmen de Guamal, Magdalena, busca mitigar los riesgos relacionados con la pérdida de Confidencialidad, Integridad y Disponibilidad de la información digital, evitando situaciones que puedan obstaculizar el logro de los objetivos estratégicos del hospital.

En este contexto, dentro del marco de Seguridad del Modelo de Seguridad y Privacidad de la Información (MSPI), la Gestión de Riesgos se convierte en un aspecto crucial en el proceso de toma de decisiones. Por tanto, esta entidad hospitalaria adopta el Plan de Tratamiento de Riesgos para evaluar las acciones necesarias que permitan mitigar los riesgos existentes en sus activos de información.

Estas acciones se organizan en forma de medidas de seguridad, conocidas como controles, y para cada uno de ellos se definen el nombre de la medida, sus objetivos, justificaciones, el responsable de su implementación y su prioridad.

	VERSION:	03
	FECHA DE ACTUALIZACION:	30-ENE-2025
PLAN DE TRATAMIENTO DE RIESGOS SEGURIDAD Y PRIVACIDAD DE LA INFORMACION	CÓDIGO:	HNSC-GG-M-012
	PAGINA	Página 4 de 24


OBJETIVOS

OBJETIVO GENERAL

Diseñar, adoptar e implementar un plan de tratamiento de riesgo de seguridad y privacidad de la información en cual permita ser una guía para el control y minimización de los riesgos con el fin de proteger la privacidad de la información de la institución.

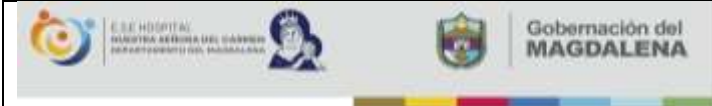
OBJETIVOS ESPECÍFICOS

- Identificar los riesgos, Amenazas y vulnerabilidades de seguridad y privacidad de la información.
- Ayudar a que las entidades logren vincular la identificación y análisis de riesgos de la entidad hacia los temas de la seguridad de la información.
- Lograr un diagnóstico real de la situación actual de la E.S.E. Hospital Nuestra Señora del Carmen de Guamal, Magdalena en materia de riesgos de seguridad y privacidad de la información.
- Reducir toda posibilidad de que una brecha o evento produzca determinado impacto bien en la información o cualquier otro activo de información asociado, a través de la gestión adecuada de los riesgos de la seguridad de la información.

	VERSION:	03
	FECHA DE ACTUALIZACION:	30-ENE-2025
PLAN DE TRATAMIENTO DE RIESGOS SEGURIDAD Y PRIVACIDAD DE LA INFORMACION	CÓDIGO:	HNSC-GG-M-012
	PAGINA	Página 5 de 24


ALCANCE

Realizar una eficiente gestión de riesgos de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación de los servicios, que permita integrar en los procesos de la entidad con buenas prácticas que contribuyan a la toma de decisiones y prevenir incidentes que puedan afectar el logro de los objetivos. Teniendo como finalidad el diagnóstico, análisis, definición y planeación del manejo de la seguridad de la información en los procesos que se ejecutan en el Hospital,; aplicando a todos los servicios del hospital, a todos sus funcionarios, contratistas, proveedores, operadores y aquellas personas o terceros que en razón del cumplimiento de sus funciones y las del hospital compartan, utilicen, recolecten, procesen, intercambien o consulten su información, así como a los entes de control, entidades relacionadas que accedan, ya sea interna o externamente a cualquier tipo de información, independientemente de su ubicación.

	VERSION:	03
	FECHA DE ACTUALIZACION:	30-ENE-2025
PLAN DE TRATAMIENTO DE RIESGOS SEGURIDAD Y PRIVACIDAD DE LA INFORMACION	CÓDIGO:	HNSC-GG-M-012
	PAGINA	Página 6 de 24

MARCO LEGAL


- **Ley 1273 de 5 de enero de 2009:** Por medio de la cual se modifica el código penal, se crea un nuevo bien jurídico tutelado denominado "DE LA PROTECCIÓN DE LA INFORMACIÓN Y DE LOS DATOS" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones entre otras disposiciones.
- **Ley 23 de 1982:** Sobre derechos de autor
- **Ley Estatutaria 1266 de 2008:** Por la cual se dictan las disposiciones generales de hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones. Para conocer más de esta Ley,
- **Ley 1581 de 2012:** la cual se dictan disposiciones generales para la Protección de Datos Personales.
- **ISO IEC 27001-2013:** Estándares internacionales sobre tecnología de la información, técnicas de seguridad, Administración de seguridad de la información, los cuales proporcionan un marco de gestión de la seguridad de la información, utilizable por cualquier tipo de empresa.
- **ISO IEC 27002-2013:** Es un estándar para la seguridad de la información.
- **Resolución 2710 de 2017.** Por la cual se establecen lineamientos para la adopción del protocolo IPv6.
- **CONPES 3995 de 2020.** Política nacional de confianza y seguridad digital, política nacional que tiene como objetivo establecer medidas para ampliar la confianza digital y mejorar la seguridad digital de manera que Colombia sea una sociedad incluyente y competitiva en el futuro digital.
- **Resolución 500 de 2021.** Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital

	VERSION:	03
	FECHA DE ACTUALIZACION:	30-ENE-2025
PLAN DE TRATAMIENTO DE RIESGOS SEGURIDAD Y PRIVACIDAD DE LA INFORMACION	CÓDIGO:	HNSC-GG-M-012
	PAGINA	Página 7 de 24


DEFINICIONES

Para la administración del riesgo, se tendrán en cuenta los siguientes términos y definiciones:

TERMINO	DEFINICIÓN
Activo de Información	Son los recursos que utiliza un Sistema de Gestión de Seguridad de la Información para que las organizaciones funcionen y consigan los objetivos que se han propuesto por la alta dirección.
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.
Amenaza	Es la causa potencial de una situación de incidente y no deseada por 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.
Causa	Son todo aquello que se pueda considerar fuente generadora de eventos (riesgos). Las fuentes generadoras o agentes generadores son las personas, los métodos, las herramientas, el entorno, lo económico, los insumos o materiales entre otros.
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.
Control	Medida que modifica el riesgo.
Criterios del riesgo	Términos de referencia frente a los cuales la importancia de un riesgo se evalúa.
Disponibilidad	Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.
Estimación del riesgo	Proceso para asignar valores a la probabilidad y las consecuencias de un riesgo.
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.
Evitación del riesgo	Decisión de no involucrarse en una situación de riesgo o tomar acción para retirarse de dicha situación.

	VERSION:	03
	FECHA DE ACTUALIZACION:	30-ENE-2025
PLAN DE TRATAMIENTO DE RIESGOS SEGURIDAD Y PRIVACIDAD DE LA INFORMACION	CÓDIGO:	HNSC-GG-M-012
	PAGINA	Página 8 de 24

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.
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 de riesgo.
Impacto	Cambio adverso en el nivel de los objetivos del negocio logrados.
Información	Corresponden a este tipo datos e información almacenada o procesada física o electrónicamente tales como: bases y archivos de datos, contratos, documentación del sistema, investigaciones, acuerdos de confidencialidad, manuales de usuario, procedimientos operativos o de soporte, planes para la continuidad del negocio, acuerdos sobre retiro y pruebas de auditoría, entre otros.
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.
Matriz de riesgos	Instrumento utilizado para ubicar los riesgos en una determinada zona de riesgo según la calificación cualitativa de la probabilidad de ocurrencia y del impacto de un riesgo.
Monitoreo	Mesa de trabajo anual, la cual tiene como finalidad, revisar, actualizar o redefinir los riesgos de seguridad de la información en cada uno de los procesos, partiendo del resultado de los seguimientos y/o hallazgos de los entes de control o las diferentes auditorías de los sistemas integrados de gestión.
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.
Política	Son instrucciones mandatorias que indican la intención de la alta gerencia respecto a la operación de la organización respecto a un asunto determinado.
Propietario del riesgo	Persona o entidad con la responsabilidad de rendir cuentas y la autoridad para gestionar un riesgo.
Recurso Informático	Elementos informáticos (base de datos, sistemas operacionales, redes, equipos de cómputo, sistemas de información y comunicaciones) que facilitan servicios informáticos.
Reducción del riesgo	Acciones que se toman para disminuir la probabilidad las consecuencias negativas, o ambas, asociadas con un riesgo.
Riesgo	Efecto de la incertidumbre sobre los objetivos.

	VERSION:	03
	FECHA DE ACTUALIZACION:	30-ENE-2025
PLAN DE TRATAMIENTO DE RIESGOS SEGURIDAD Y PRIVACIDAD DE LA INFORMACION	CÓDIGO:	HNSC-GG-M-012
	PAGINA	Página 9 de 24

Riesgo en la seguridad de la información	Potencial de que una amenaza determinada explote las vulnerabilidades de los activos o grupos de activos causando así daño a la organización.
Riesgo Inherente	Es el nivel de riesgo propio de la actividad, sin tener en cuenta el efecto de los controles.
Riesgo Residual	El riesgo que permanece tras el tratamiento del riesgo o nivel resultante del riesgo después de aplicar los controles.
Seguimiento	Mesa de trabajo semestral, en el cual se revisa el cumplimiento del plan de acción, indicadores y metas de riesgo y se válida la aplicación n de los controles de seguridad de la información sobre cada uno de los procesos.
Seguridad de la información	Preservación de la confidencialidad, integridad y disponibilidad de la información.
Software	Se conoce como al soporte lógico de un sistema informático, que comprende el conjunto de los componentes lógicos necesarios que hacen posible la realización de tareas específicas, en contraposición a los componentes físicos que son llamados hardware
Tratamiento del Riesgo	Proceso para modificar el riesgo” (Icontec Internacional, 2011).
Valoración del Riesgo	Proceso global de identificación del riesgo, análisis del riesgo y evaluación de los riesgos.
Vulnerabilidad	Es aquella debilidad de un activo o grupo de activos de información.


DIRECCIONAMIENTO ESTRATEGICO E.S.E. HOSPITAL NUESTRA SEÑORA DEL CARMEN DE GUAMAL, MAGDALENA.

IDENTIFICACION GENERAL

La E.S.E. Hospital Nuestra Señora del Carmen de Guamal es una entidad de naturaleza pública, descentralizada, con personería jurídica, patrimonio propio y autonomía administrativa, adscrita a la Dirección Departamental del Sistema de Seguridad Social en Salud, y sometida al régimen jurídico previsto en el Capítulo 03, Artículos 194, 195 y 197 de la Ley 100 de 1.993 y sus decretos reglamentarios, y demás disposiciones que lo modifiquen, adicionen, reformen o sustituyan. El domicilio y sede de sus organismos administrativos, se encuentra ubicados, en la Calle 10 Carrera 5a Esquina, su jurisdicción comprende todo el territorio del Municipio de Guamal, Departamento del Magdalena

MISIÓN

Nuestra misión es proporcionar atención médica integral oportuna, a todos los ciudadanos del municipio de Guamal - Magdalena, con un enfoque especial en la promoción y prevención

	VERSION:	03
	FECHA DE ACTUALIZACION:	30-ENE-2025
PLAN DE TRATAMIENTO DE RIESGOS SEGURIDAD Y PRIVACIDAD DE LA INFORMACION	CÓDIGO:	HNSC-GG-M-012
	PAGINA	Página 10 de 24

de la salud. Llevando a cabo la eficiencia y eficacia, para dar cumpliendo a los estándares de calidad, logrando la máxima satisfacción y seguridad del paciente

VISIÓN

La E.S.E. Hospital Nuestra Señora del Carmen para el 2028 se visualiza como un líder de excelencia en atención médica, con un modelo de gestión humanizado, seguro e integral. Como prestador primario al posicionarse en el cumplimiento más alto de estándares de calidad. Contribuyendo al mejoramiento de la salud y bienestar de los clientes internos y externos.

ROL DE LA E.S.E DENTRO DE LA RED DEPARTAMENTAL

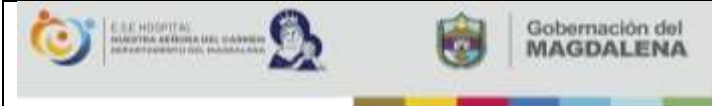
La Red de prestación de servicios de salud del Departamento del Magdalena, se encuentra organizada en cinco subregiones, teniendo en cuenta los criterios de localización geográfica, vocación económica, división político-administrativa y vínculos intermunicipales, las cuales se agrupan en 29 municipios, y el Distrito Turístico, Cultural e Histórico de Santa Marta, se encuentra organizada por subregiones. Dichas subregiones son: subregión Norte, subregión Centro, subregión Río y la subregión Sur; con tres niveles de complejidad: baja, mediana y alta.

La E.S.E Hospital Nuestra Señora del Carmen de Guamal, de acuerdo al Documento de Red en el Programa Territorial de Reorganización, Rediseño y Modernización de Redes de Empresas Sociales del Estado del Departamento del Magdalena, es una institución de Baja Complejidad, Categoría tipo C; ubicada en la subregión sur; habilitada según el REPS, con única sede de prestación de servicios.

La E.S.E Hospital "Nuestra Señora del Carmen" hace parte de la Subregión Sur de la Red de Servicios de Salud del Departamento del Magdalena, integrada por los municipios de: El Banco, Guamal, San Sebastián de Buena Vista, Santa Bárbara de Pinto, Pijiño del Carmen, San Zenón y Santa Ana.

En la subregión Sur, se cuenta con cinco (5) E.S.E de baja complejidad, de carácter Departamental, en los municipios de Guamal, San Sebastián de Buena Vista, San Zenón, Santa Bárbara de Pinto, Pijiño del Carmen y dos (2) ESE de baja complejidad del carácter Municipal, la ESE Hospital Local Nuestra Señora de Santa Ana en el municipio de Santa Ana y la ESE Hospital Samuel Villanueva Valest en el municipio de El Banco.

Sus centros de referencia para mediana complejidad natural, es la E.S.E. Hospital La Candelaria del municipio de El Banco (Magdalena), y la red complementaria, es la E.S.E. Hospital Universitario del Caribe con sede en Mompo (Bolívar); y para la alta complejidad, la E.S.E. Hospital Universitario Fernando Troconis y Clínicas de la Red Privada del Distrito de Santa Marta.

	VERSION:	03
	FECHA DE ACTUALIZACION:	30-ENE-2025
PLAN DE TRATAMIENTO DE RIESGOS SEGURIDAD Y PRIVACIDAD DE LA INFORMACION	CÓDIGO:	HNSC-GG-M-012
	PAGINA	Página 11 de 24

PRESTACION DE LOS SERVICIOS

Por la condición especial del municipio de Guamal, en el cual, el 71% de la población es de asentamiento rural disperso, nuestra institución basa su modelo de atención integral, bajo modalidades de medicina asistencial preventiva, con énfasis en Atención Primaria; en razón que sus atenciones se están generando a nivel de los corregimientos con un modelo de penetración con cubrimiento a la población rural, al no disponer de infraestructura física y las condiciones mínimas de un espacio adecuado para la atención de esta población.

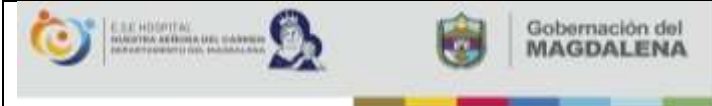
Este modelo de prestación de servicios, se ha fortalecido a partir de la vigencia 2013, teniendo en cuenta que, en el municipio de Guamal, las secuelas dejadas por el conflicto armado interno, impactaron negativamente en la ejecución de actividades direccionadas en las penetraciones asistenciales de salud, para la asistencia de la población vulnerable del área rural de asentamiento disperso.

Además de hacer esfuerzos en optimizar la calidad de la prestación de los servicios de salud, en lo que respecta a la atención primaria, limitamos el incremento de la demanda de algunos servicios que le generan a la entidad altos costos y barreras de accesibilidad para garantizar la oportunidad de la atención del usuario, tal es el caso del servicio de urgencias, en el que se puede ver involucrado el servicio de Transporte Asistencial Básico, esto teniendo en cuenta las deficiencias en los medios de transporte, especialmente de vías terrestres, teniendo en cuenta, el recorrido de largas distancias, y el mal estado de la estructura de la malla vial, aunado a las condiciones climáticas, teniendo en cuenta que en períodos de invierno, empeoran las condiciones de dichos traslados.

VALORES INSTITUCIONALES

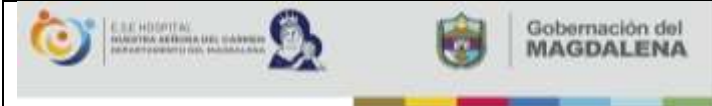
La E.S.E. Hospital Nuestra Señora del Carmen de Guamal – Magdalena, tiene establecido en su Código de Ética y Buen Gobierno el marco de la filosofía del servicio que presta, las normas morales y éticas, además de los valores cotidianos que se constituyen en las creencias que nos unen en torno a nuestros usuarios y partes interesadas, y a través de ello, se rige la conducta y actuar de cada integrante de la E.S.E los cuales se recogen en los siguientes valores:

- **INNOVACIÓN:** Es la capacidad del hospital para implementar nuevas ideas, tecnologías y procesos que mejoren la calidad de los servicios de salud, optimicen la atención al paciente y se adapten a las demandas cambiantes del sector. Este valor impulsa el progreso constante, fomenta la creatividad y asegura que la institución se mantenga a la vanguardia en el cuidado médico.
- **INCLUSIÓN:** Compromiso del hospital con la equidad y el respeto a la diversidad, garantizando que todas las personas, independientemente de su origen, condición

	VERSION:	03
	FECHA DE ACTUALIZACION:	30-ENE-2025
PLAN DE TRATAMIENTO DE RIESGOS SEGURIDAD Y PRIVACIDAD DE LA INFORMACION	CÓDIGO:	HNSC-GG-M-012
	PAGINA	Página 12 de 24

social, género, religión, discapacidad u otras características, recibirán atención médica de calidad en un entorno accesible, respetuoso y libre de discriminación.

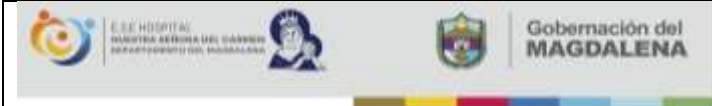
- **SOSTENIBILIDAD:** El compromiso del hospital de gestionar sus recursos de manera responsable, equilibrando las necesidades actuales con la protección del medio ambiente y el bienestar de las generaciones futuras. Esto incluye implementar prácticas ecológicas, optimizar el uso de energía y materiales, y garantizar la viabilidad económica y social de los servicios de la ese.
- **RESPONSABILIDAD SOCIAL:** El compromiso del hospital de contribuir al desarrollo integral de la comunidad, más allá de la atención médica, a través de acciones que promuevan el bienestar social, la educación en salud, la prevención de enfermedades y el apoyo a poblaciones vulnerables. Este valor refleja la ética de la institución en generar un impacto positivo y sostenible en el entorno social en el que opera.
- **COMPETITIVIDAD:** La capacidad del hospital para destacarse en el sector de la salud mediante la excelencia en sus servicios, la implementación de tecnologías avanzadas, la mejora continua de sus procesos y la formación de un equipo humano altamente calificado. Este valor garantiza que la institución se mantenga a la vanguardia, ofreciendo soluciones innovadoras y de calidad que satisfagan las necesidades de los pacientes y superen sus expectativas.
- **SEGURIDAD:** Hace referencia a la creación de un entorno seguro tanto para los pacientes como para los empleados del hospital. Implica la adopción de protocolos para prevenir errores médicos, infecciones y accidentes, garantizando la protección y el bienestar de todos los involucrados.
- **EXCELENCIA:** es el compromiso de proporcionar una atención sanitaria de la más alta calidad, de manera eficiente, ética y compasiva, utilizando las mejores prácticas médicas y las tecnologías más avanzadas. Se basa en un enfoque integral que abarca desde la gestión administrativa hasta la atención directa al paciente, promoviendo siempre la mejora continua.
- **ÉTICA:** el conjunto de valores y principios que orientan las acciones y decisiones dentro de un hospital, asegurando que se actúe con justicia, integridad, respeto por los derechos humanos, y en cumplimiento con las leyes y regulaciones vigentes. La ética médica y hospitalaria se enfoca especialmente en el respeto a la autonomía del paciente, la confidencialidad, la justicia y el cuidado compasivo, todo dentro de un marco de responsabilidad profesional.

	VERSION:	03
	FECHA DE ACTUALIZACION:	30-ENE-2025
PLAN DE TRATAMIENTO DE RIESGOS SEGURIDAD Y PRIVACIDAD DE LA INFORMACION	CÓDIGO:	HNSC-GG-M-012
	PAGINA	Página 13 de 24

- **HUMANIDAD:** un valor esencial que va más allá del tratamiento técnico de enfermedades, reconociendo que los pacientes son seres humanos con necesidades emocionales, sociales y espirituales. La humanidad en la atención hospitalaria se refleja en la empatía, el respeto, la dignidad y el apoyo emocional brindado a cada paciente. Este enfoque integral no solo mejora la calidad del cuidado, sino que también promueve la recuperación, la confianza y el bienestar general del paciente y sus seres queridos.
- **COLABORACIÓN:** es fundamental para ofrecer atención de calidad y eficaz. Implica que todos los miembros del equipo de salud trabajen de manera conjunta, compartiendo información, respetándose mutuamente y coordinando esfuerzos para brindar la mejor atención posible a los pacientes. Esta cooperación no solo mejora la calidad de los cuidados y los resultados clínicos, sino que también crea un ambiente de trabajo más positivo y eficiente, y favorece una experiencia del paciente más satisfactoria y segura.
- **RESPONSABILIDAD:** es un valor fundamental que asegura que cada miembro del equipo de salud y del personal hospitalario cumpla con sus deberes de manera profesional, ética y eficiente. Va más allá de la acción individual e incluye la rendición de cuentas tanto ante los pacientes como ante la institución hospitalaria.


PRINCIPIOS INSTITUCIONALES

- **CALIDAD:** La calidad en la atención hospitalaria se refiere a la entrega de servicios de salud de alta calidad que sean eficaces, eficientes, seguras, accesibles y centrados en el paciente. Implica no solo cumplir con los estándares médicos, sino también asegurar una experiencia positiva para el paciente.
- **OPORTUNIDAD:** garantizar que los pacientes reciban la atención médica adecuada en el momento adecuado, lo que puede ser crucial para la prevención de enfermedades graves, la mejora de los resultados clínicos y la satisfacción del paciente.
- **INTEGRALIDAD:** segura una atención completa, coordinada y centrada en el paciente, considerando todas las dimensiones de su salud, desde lo físico hasta lo psicológico y social. Este enfoque tiene como objetivo ofrecer un tratamiento adecuado, personalizado y continuo, promoviendo la prevención, la mejora de la calidad de vida y una recuperación más efectiva.
- **ACCESIBILIDAD:** La accesibilidad se refiere a la capacidad de las personas para obtener atención médica oportuna sin barreras económicas, geográficas, sociales o

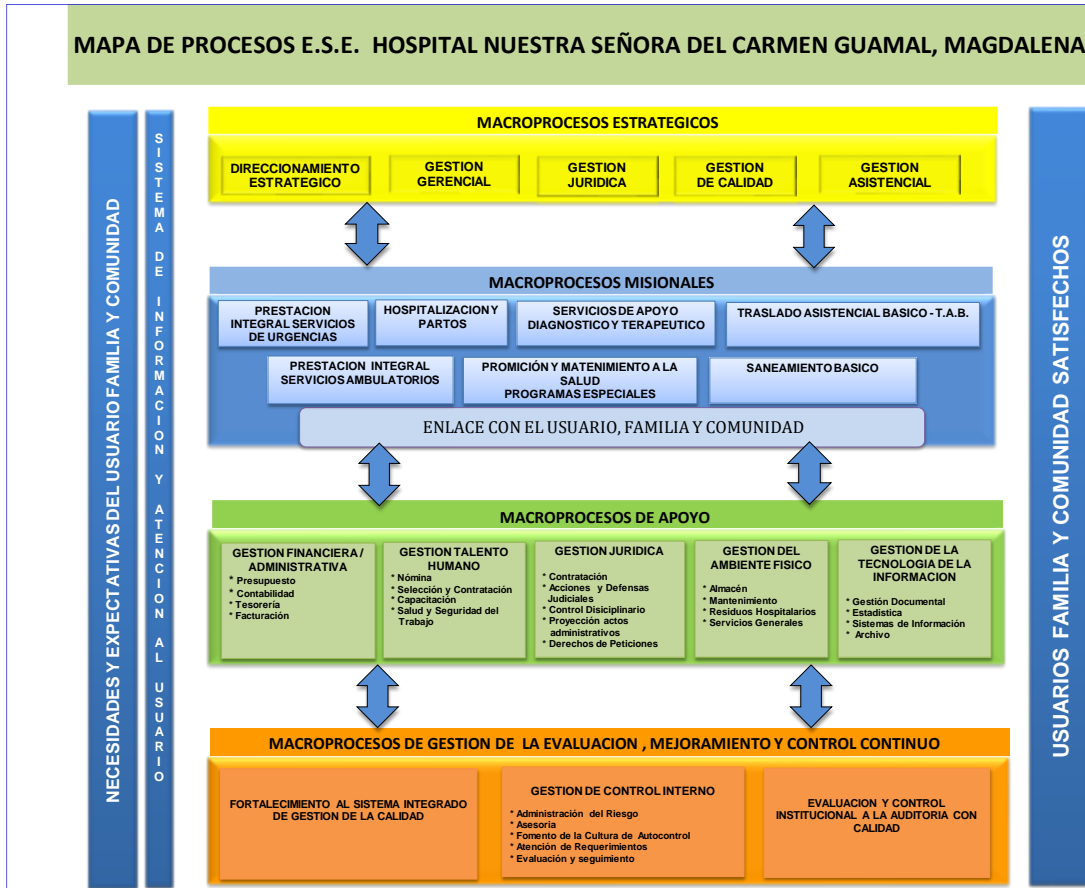
	VERSION:	03
	FECHA DE ACTUALIZACION:	30-ENE-2025
PLAN DE TRATAMIENTO DE RIESGOS SEGURIDAD Y PRIVACIDAD DE LA INFORMACION	CÓDIGO:	HNSC-GG-M-012
	PAGINA	Página 14 de 24


culturales. Los hospitales deben ser accesibles a toda la población, asegurando que todos los pacientes tengan igual oportunidad de recibir atención adecuada.

- **EFFECTIVIDAD:** asegura que los tratamientos, cuidados y servicios proporcionados logren los resultados esperados, mejorando la salud del paciente, optimizando los recursos y minimizando complicaciones. Implica la aplicación de prácticas basadas en la evidencia, el uso eficiente de recursos, la atención integral y un enfoque preventivo.
- **EFICIENCIA:** es un principio clave que asegura que los recursos disponibles (humanos, materiales, tecnológicos, financieros) se utilicen de la manera más óptima para alcanzar los mejores resultados en la salud de los pacientes, sin desperdiciar tiempo ni costos. Implica mejorar los procesos, reducir tiempos de espera, utilizar la tecnología para automatizar tareas, y aplicar un enfoque preventivo.
- **HUMANIZACIÓN:** implica un enfoque integral que pone al paciente en el centro de la atención, respetando su dignidad, sus emociones, sus valores y sus necesidades individuales. Involucra un trato respetuoso, empático y compasivo, y promueve un ambiente de confianza, donde tanto los pacientes como sus familias se sienten apoyados en todas las dimensiones
- **CONFIANZA:** Entregaremos esperanza y seguridad en nuestro actuar.

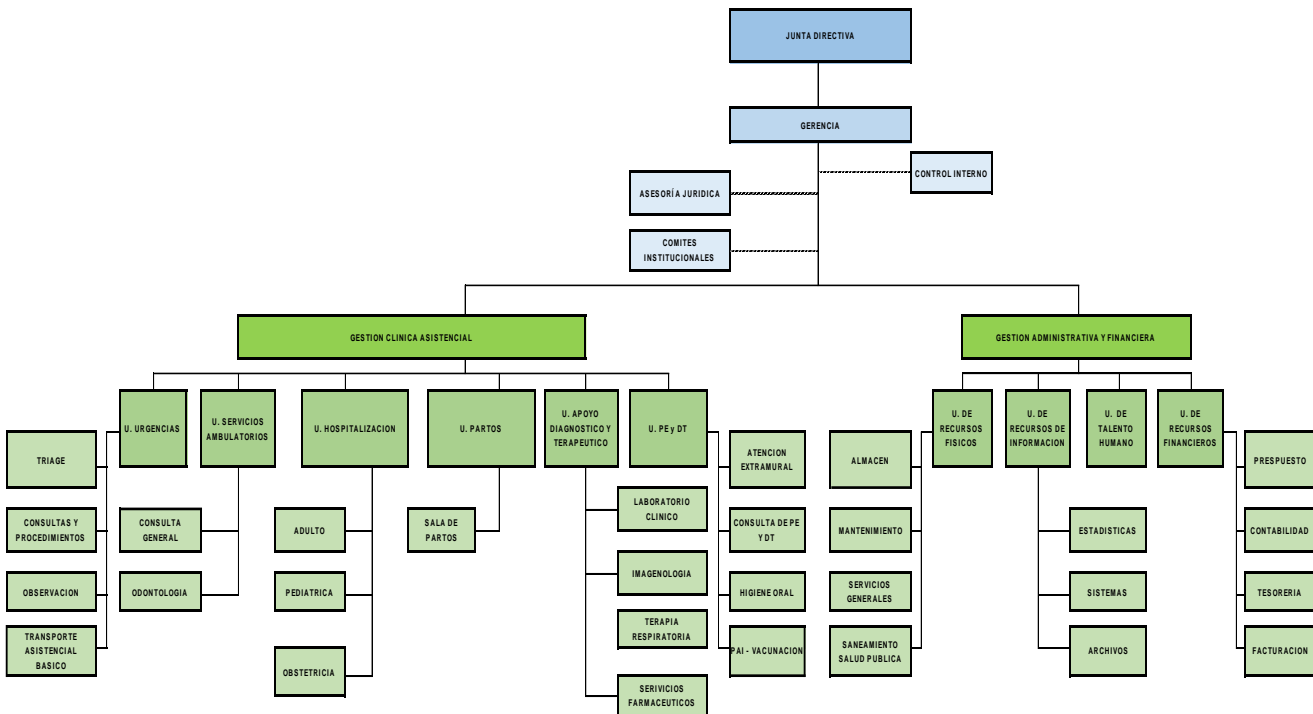
	VERSION:	03
	FECHA DE ACTUALIZACION:	30-ENE-2025
PLAN DE TRATAMIENTO DE RIESGOS SEGURIDAD Y PRIVACIDAD DE LA INFORMACION	CÓDIGO:	HNSC-GG-M-012
	PAGINA	Página 15 de 24


MAPA DE PROCESOS



	VERSION:	03
	FECHA DE ACTUALIZACION:	30-ENE-2025
PLAN DE TRATAMIENTO DE RIESGOS SEGURIDAD Y PRIVACIDAD DE LA INFORMACION	CÓDIGO:	HNSC-GG-M-012
	PAGINA	Página 16 de 24

ORGANIGRAMA




	VERSION:	03
	FECHA DE ACTUALIZACION:	30-ENE-2025
PLAN DE TRATAMIENTO DE RIESGOS SEGURIDAD Y PRIVACIDAD DE LA INFORMACION	CÓDIGO:	HNSC-GG-M-012
	PAGINA	Página 17 de 24

OFERTA DE SERVICIOS DE LA E.S.E. HOSPITAL NUESTRA SEÑORA DEL CARMEN DE GUAMAL – MAGDALENA

PORTAFOLIO DE SERVICIOS

La E.S.E. Hospital Nuestra Señora del Carmen de Guamal, Magdalena, como Prestador de Servicios de Salud de baja complejidad, identificada con el REPS 473180024501, según Constancia de Habilitación en el Registro Especial de Prestadores de Servicios de Salud, emitida por la Secretaría de Salud del Magdalena, el día 27 de diciembre de 2024, se encuentra habilitada para prestar los servicios declarados en el formulario de inscripción, con los siguientes datos generales.

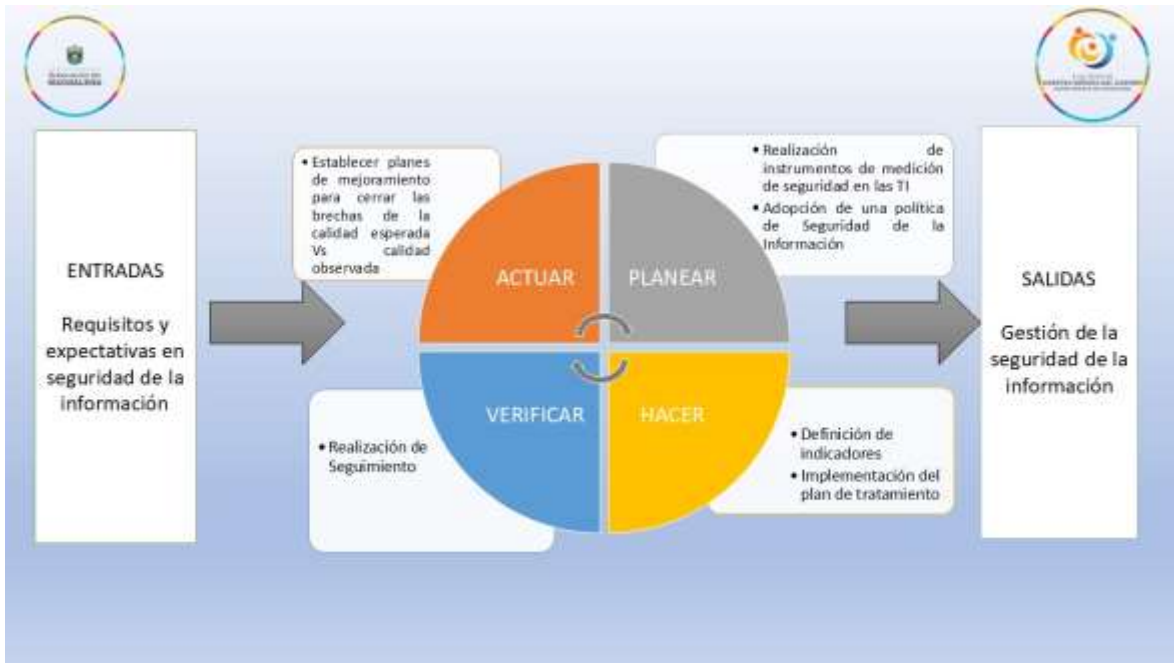
GRUPO DEL SERVICIO	COD SER	NOMBRE SERVICIO
INTERNACIÓN	129	Hospitalización adultos
INTERNACIÓN	130	Hospitalización pediátrica
CONSULTA EXTERNA	312	Enfermería
CONSULTA EXTERNA	328	Medicina general
CONSULTA EXTERNA	333	Nutrición dietética
CONSULTA EXTERNA	324	Odontología general
CONSULTA EXTERNA	344	Psicología
CONSULTA EXTERNA	420	Vacunación
ATENCIÓN INMEDIATA	1102	Urgencias
ATENCIÓN INMEDIATA	1103	Transporte asistencial básico
ATENCIÓN INMEDIATA	1101	Atención del parto
APOYO DIAGNÓSTICO Y COMPLEMENTACIÓN TERAPÉUTICA	706	Laboratorio clínico
APOYO DIAGNÓSTICO Y COMPLEMENTACIÓN TERAPÉUTICA	712	Toma de muestras de laboratorio clínico
APOYO DIAGNÓSTICO Y COMPLEMENTACIÓN TERAPÉUTICA	714	Servicio farmacéutico
APOYO DIAGNÓSTICO Y COMPLEMENTACIÓN TERAPÉUTICA	729	Terapia respiratoria
APOYO DIAGNÓSTICO Y COMPLEMENTACIÓN TERAPÉUTICA	739	Fisioterapia
APOYO DIAGNÓSTICO Y COMPLEMENTACIÓN TERAPÉUTICA	744	Imágenes diagnosticas – ionizantes
APOYO DIAGNÓSTICO Y COMPLEMENTACIÓN TERAPÉUTICA	749	Tamización de cáncer de cuello uterino

	VERSION:	03
	FECHA DE ACTUALIZACION:	30-ENE-2025
PLAN DE TRATAMIENTO DE RIESGOS SEGURIDAD Y PRIVACIDAD DE LA INFORMACION	CÓDIGO:	HNSC-GG-M-012
	PAGINA	Página 18 de 24


DESARROLLO DEL TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Para el desarrollo de este plan, resulta fundamental contar con la participación activa de los miembros directivos y representantes de las áreas asistenciales. Su presencia garantiza que la información más relevante de la entidad esté disponible de manera oportuna. Esto permite impulsar un enfoque transversal en toda la organización hospitalaria, evitando que la responsabilidad recaiga únicamente en la oficina o área de Tecnología de la Información.

Para llevar a cabo este propósito, se basará la estrategia en el modelo PHVA.



FASE	DESCRIPCIÓN
PLANEACIÓN	Se realizarán instrumentos de medición para medir la seguridad de la información Se desarrollará y adoptará la Política de Seguridad de la Información
HACER	En esta fase implantaran los indicadores, diseñados en la fase de planeación. Implementará y socializará la política de Seguridad de la Información

	VERSION:	03
	FECHA DE ACTUALIZACION:	30-ENE-2025
PLAN DE TRATAMIENTO DE RIESGOS SEGURIDAD Y PRIVACIDAD DE LA INFORMACION	CÓDIGO:	HNSC-GG-M-012
	PAGINA	Página 19 de 24

VERIFICAR	Se harán seguimientos Trimestrales para ver la trazabilidad de los indicadores
HACER	Al no cumplimiento de los indicadores, se deberá realizar un plan de mejoramiento.

Para planear y gestionar la implementación del de plan de tratamiento de seguridad y privacidad de la información se contará con un grupo interdisciplinario que será liderado por el responsable de seguridad de la información del hospital quien deberá entregar y dar a conocer los perfiles y responsabilidades de cada persona al grupo de trabajo e identificar las personas idóneas para asignar cada rol.

VALORACIÓN DEL RIESGO

Para la identificación y evaluación se toma como base el contexto estratégico que reconoce las situaciones de riesgo de origen interno y externo para la entidad; luego se procede a la identificación de los riesgos, reconociendo variables como agentes generadores, causas, efectos entre otros, para realizar posteriormente la calificación de los riesgos. A partir de los factores internos y externos, se determinan los agentes generadores del riesgo de seguridad y privacidad de la información sus causas y sus consecuencias: pérdida, daño, perjuicio o detrimento.

Para los riesgos de seguridad y privacidad se debe tener en cuenta:

IDENTIFICACIÓN DEL RIESGO


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.

IDENTIFICACIÓN DE LOS ACTIVOS

Según la norma ISO 27000:2013 un activo es todo aquello que tiene valor para la entidad y que, por lo tanto, requiere de protección. La identificación de activos se debería llevar a cabo con un nivel adecuado de detalle que proporcione información suficiente para la valoración del riesgo.

IDENTIFICACIÓN DE LAS AMENAZAS

Una amenaza tiene el potencial de causar daños a activos tales como información, procesos y sistemas y, por lo tanto, a la entidad. Las amenazas pueden ser de origen natural o humano y podrían ser accidentales o deliberadas es recomendable identificar todos los orígenes de las amenazas accidentales como deliberadas. Las amenazas se deberían identificar genéricamente y por tipo (ej. Acciones no autorizadas, daño físico, fallas técnicas)

	VERSION:	03
	FECHA DE ACTUALIZACION:	30-ENE-2025
PLAN DE TRATAMIENTO DE RIESGOS SEGURIDAD Y PRIVACIDAD DE LA INFORMACION	CÓDIGO:	HNSC-GG-M-012
	PAGINA	Página 20 de 24

Algunas amenazas pueden afectar a más de un activo y en tales casos pueden causar diferentes impactos dependiendo de los activos que se vean afectados.


IDENTIFICACIÓN DE CONTROLES EXISTENTES

Se debe realizar la identificación de los controles existentes para evitar trabajo o costos innecesarios, por ejemplo, la duplicidad de controles, además de esto mientras se identifican los controles se recomienda hacer una verificación para garantizar que los existentes funcionan correctamente.


IDENTIFICACIÓN DE LAS VULNERABILIDADES

Para realizar una correcta identificación de vulnerabilidades es necesario conocer la lista de amenazas comunes, la lista de inventario de activos y el listado de controles existentes. Se pueden identificar vulnerabilidades en las siguientes áreas:

- ✓ Organización.
- ✓ Procesos y procedimientos.
- ✓ Rutinas de gestión.
- ✓ Personal
- ✓ Ambiente físico
- ✓ Configuración del sistema de información.
- ✓ Hardware, software y equipos de comunicaciones.
- ✓ Dependencia de partes externas.

	VERSION:	03
	FECHA DE ACTUALIZACION:	30-ENE-2025
PLAN DE TRATAMIENTO DE RIESGOS SEGURIDAD Y PRIVACIDAD DE LA INFORMACION	CÓDIGO:	HNSC-GG-M-012
	PAGINA	Página 21 de 24

IDENTIFICACION DEL RIESGO				
EVENTO	CAUSA DEL RIESGO		CONSECUENCIA	ACCIÓN
	INTERNO	EXTERNO		
Interrupción de la operación del sistema de información	Caída del sistema hacia los servidores Obsolescencia tecnológica de los equipos. Daños por falta de mantenimiento en los equipos.	Caída del fluido eléctrico Pérdida de señal a internet por parte de la red Falta de equipos o servidores Daños físicos por caídas de equipos o de alimentos	Congestión o no continuidad en la atención por fallas en la red Pérdida de información a causa de la contingencia.	Constante mantenimientos de equipos de cómputo. Mantenimiento en la red y el sistema.
Pérdida de información	Fallas en las copias de seguridad. Falta de sistemas para hacer los backup Falta de Disco duros para realizar las copias de seguridad	Fallas en los fluidos eléctricos. Fallas de los equipos de cómputo Falta de conocimiento para hacer los Backup	Pérdida de información clasificada Pérdida de base de datos personales.	Implementación de un backup para la protección de datos personales Capacitación al personal para el debido respaldo de datos personales
Manipulación incorrecta de historia clínica	Caída del sistema en los servidores Falta de conexión al	Historias clínicas incompletas.	Retraso en la atención Entrega de Historias clínicas incompletas	Auditoria de historias clínicas. capacitación a personal médico para



	VERSION:	03
	FECHA DE ACTUALIZACION:	30-ENE-2025
PLAN DE TRATAMIENTO DE RIESGOS SEGURIDAD Y PRIVACIDAD DE LA INFORMACION	CÓDIGO:	HNSC-GG-M-012
	PAGINA	Página 22 de 24

	momento de guardar la HC			correcto diligenciamiento de historias clínicas Mantenimiento de la red
--	--------------------------	--	--	--


En base a la identificación del riesgo y el ciclo PHVA planteado se realiza el siguiente cronograma.

CRONOGRAMA

ACTIVIDAD	RESPONSABLE	VIGENCIA 2025			
		I TRIMESTRE	II TRIMESTRE	III TRIMESTRE	IV TRIMESTRE
Adopción de la política Seguridad de la Información	Gerencia Quien delegue				
Realización de Instrumentos de medición de Seguridad	Gerencia Calidad				
Identificación y actualización de activos de información	Gerencia Calidad				
Cronograma de mantenimiento de equipos de computo	Gerencia Calidad Ing electrónico contratado				
Capacitación al personal para el debido respaldo de datos personales	Gerencia Calidad Ing electrónico contratado				
Implantarán los indicadores, diseñados en la fase de planeación.	Gerencia Calidad				

 	VERSION:	03
	FECHA DE ACTUALIZACION:	30-ENE-2025
PLAN DE TRATAMIENTO DE RIESGOS SEGURIDAD Y PRIVACIDAD DE LA INFORMACION	CÓDIGO:	HNSC-GG-M-012
	PAGINA	Página 23 de 24

Implementará y socializará la política de Seguridad de la Información	Gerencia Calidad				
Verificación de la información de la implementación	Gerencia Calidad				
Auditoria de historias clínicas	Comité de HC				
capacitación a personal médico para correcto diligenciamiento de historias clínicas	Comité de HC				
Realización y socialización de plan de mejoramientos para cerrar brechas	Gerencia Calidad				

	VERSION:	03
	FECHA DE ACTUALIZACION:	30-ENE-2025
PLAN DE TRATAMIENTO DE RIESGOS SEGURIDAD Y PRIVACIDAD DE LA INFORMACION	CÓDIGO:	HNSC-GG-M-012
	PAGINA	Página 24 de 24

BIBLIOGRAFÍA.

https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-162621_Modelo_de_Seguridad_y_Privacidad_MSPI.pdf

<https://www1.funcionpublica.gov.co/web/mipg/detalle-del-modelo/tags/dimension-gestion-conocimiento>

<https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Estrategias/MSPI/>