1. INTRODUCCIÓN

La información que genera constantemente La **ESE Hospital Rosario Pumarejo de López**, es crucial para su correcto desempeño y cumplimiento de los objetivos organizacionales, es por ello que la seguridad y privacidad de la información se convierten en atributos indispensables para evitar cualquier posibilidad de alteración, mal uso, pérdida, entre otros eventos, que puedan significar una alteración para el normal desarrollo en la prestación de servicios de salud.

De acuerdo a lo mencionado anteriormente, dentro del Marco de Seguridad del Modelo de Seguridad y Privacidad de la información –MSPI-, un tema decisivo, es la Gestión de riesgos la cual es utilizada para la toma de decisiones. Es por esto que La **ESE Hospital Rosario Pumarejo de López**, adopta la metodología “Guía de Riesgos” del Departamento Administrativo de la Función Púbica y como herramienta metodológica la utilizada por la Unidad Nacional para la Gestión del Riesgo de Desastres de la Presidencia de la República, además ha incorporado como referente la Norma ISO 31000 con el objetivo de generar buenas prácticas de gobierno corporativo y del mejoramiento continuo en la gestión de riesgos.

La **ESE Hospital Rosario Pumarejo de López**, acoge la gestión de riesgos como un proceso sistemático de identificación, análisis, evaluación, valoración, y tratamiento de los riesgos; aplicando los controles necesarios para evitar, reducir, compartir, transferir o asumir el riesgo con medidas preventivas o correctivas que deberá generar como resultado minimizar pérdidas, maximizar rendimientos y cuidar la seguridad del paciente.

2. RESPONSABLES:

La estructura organizacional de los procesos responsables de la implementación del plan es la siguiente:

- Subgerente Administrativo y Financiero
- Asesor planeación, calidad y sistemas de información
- Profesional líder Calidad
- Profesional Universitario Sistemas
- Líder de gestión documental
- Profesional Especializado Estadística

3. PLATAFORMA ESTRATÉGICA:

3.1. IDENTIFICACIÓN Y NATURALEZA:

El Hospital Rosario Pumarejo de López es una Empresa Social del Estado, de conformidad con lo establecido en la Ordenanza N° 048 del 10 de diciembre de 1994, con categoría especial de entidad pública descentralizada del orden departamental, dotada de personería jurídica, patrimonio propio y autonomía administrativa, con una oferta de servicios de salud de mediana complejidad para atender la población del Departamento del Cesar y sus zonas de influencia, que presta sus servicios en la única sede ubicada la ciudad de Valledupar.

3.2. MISIÓN:

La ESE Hospital Rosario Pumarejo de López presta servicios Integrales de salud de mediana y alta complejidad en el Departamento del Cesar y su área de influencia, con talento humano idóneo comprometido con el mejoramiento continuo, la atención segura, humanizada, centrada en el usuario, la familia en su contexto multiétnico y cultural fortalecido con la relación docencia Servicio y la sostenibilidad financiera y ambiental.

3.3. VISIÓN:

La ESE Hospital Rosario Pumarejo de López en el 2027, será una institución referente en el departamento del Cesar y su área de influencia, auto sostenible financieramente, con un equipo humano calificado y orientado a la acreditación de servicios integrales de salud de alta complejidad y a la transformación como hospital Universitario.

3.4. PRINCIPIOS ÉTICOS:

Humanización del servicio: proporcionamos los cuidados a los usuarios de manera solidaria, digna, con respeto, empatía, teniendo en cuenta sus decisiones y sus valores.

Pertinencia: brindamos a los usuarios los servicios de salud que requieren según criterio médico.

Oportunidad: prestamos servicios de salud a nuestros usuarios sin retrasos que pongan en riesgo la salud y vida.

Seguridad: prestamos servicios de salud bajo protocolos y lineamientos orientados a prevenir la ocurrencia de un evento adverso.

Trabajo en equipo: nuestros funcionarios y contratistas articulan sus habilidades, dones

y talentos con los lineamientos institucionales para alcanzar las metas y lograr los objetivos.

3.5. VALORES INSTITUCIONALES – CÓDIGO DE INTEGRIDAD:

Respeto: Reconozco, valoro y trato de manera digna a todas las personas, con sus virtudes y defectos, sin importar su labor, se procedencia, títulos o cualquier otra condición.

Honestidad: Actúo siempre con fundamento en la verdad, cumpliendo mis deberes con transparencia y rectitud, y siempre favoreciendo el interés general.

Compromiso: Soy consciente de la importancia de mi rol como servidor público y estoy en disposición permanente para comprender y resolver las necesidades de las personas con las que me relaciono en mis labores cotidianas, buscando siempre mejorar su bienestar.

Diligencia: Cumplo con los deberes, funciones y responsabilidades asignadas a mi cargo de la mejor manera posible, con atención, prontitud, destreza y eficiencia, para así optimizar el uso de los recursos del Estado.

Justicia: Actúo con imparcialidad garantizando los derechos de las personas, con equidad, igualdad y sin discriminación.

4. GLORARIO

Amenazas: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.

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 auditoria y obviamente para determinar el grado en el que se cumplen los criterios de auditoria.

Ley de Transparencia y Acceso a la Información Pública: Se refiere a la Ley Estatutaria 1712 de 2014.

Activos de información: Elementos de Hardware y de Software de

procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de cada entidad, órgano u organismo.

Este tipo de activo representa los datos de la organización, información que tiene valor para los procesos de negocio, independientemente de su ubicación: puede ser un documento físico debidamente firmado, un archivo guardado en un servidor, un aplicativo o cualquier elemento que permita almacenar información valiosa o útil para el Hospital Rosario Pumarejo de López.

Comité de Seguridad de la Información (CSI): Instancia del nivel superior, que deben validar la Política de Información, así como los procesos, procedimientos y metodologías específicas de seguridad de la información para el adecuado uso y administración de los recursos informáticos y físicos, asignados a los servidores públicos de cada ente público. Para la E.S.E. Hospital Rosario Pumarejo de López, se tiene el Comité Institucional de Gestión y Desempeño, el cual asume a través de la dimensión de Información y Comunicación, las funciones del CSI.

Confidencialidad: Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

Control: Es toda actividad o procesos encaminado a mitigar o evitar un riesgo. Incluye políticas, procedimientos, guías, estructuras organizacionales, buenas prácticas que pueden ser de carácter administrativo, técnico o legal.

Disponibilidad: Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.

Evento de seguridad de la información: Se considera un Evento de Seguridad de la Información a cualquier situación identificada que indique una posible brecha en la Política de Información o falla en los controles y/o protecciones establecidas.

Incidente de seguridad de la información: Un incidente de seguridad de la información se define como un acceso, uso, divulgación, modificación o destrucción no autorizada de la información de Hospital Rosario Pumarejo de López y de sus usuarios; un impedimento en la operación normal de las redes, sistemas o recursos informáticos; o cualquier otro acto que implique una violación

a la Política de Información.

Integridad: Propiedad de salvaguardar la exactitud y estado completo de los activos.

Propietario/responsable de activo de información: Individuo, entidad o unidad de negocio que ha aceptado la responsabilidad de la administración para el control, producción, desarrollo, mantenimiento, uso y seguridad de los activos de información.

Servicio: Es cualquier acto o desempeño que una persona puede ofrecer a otra que es esencialmente intangible y que no conlleva ninguna propiedad. Su producción puede o no estar ligada a un producto físico.

Usuario: Es el nombre (o alias) que se le asigna a cada persona para ser identificado por el servidor, de esta manera el proveedor de Internet o de correo electrónico lo identifica, es única en cada servidor, y cada usuario tiene asignado una contraseña para poder acceder a su cuenta.

5. DESARROLLO DEL PLAN

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, dónde, y por qué podría ocurrir está perdida, las siguientes etapas recolectan datos de entrada para esta actividad.

Normalmente se identifican los riesgos como eventos o situaciones no deseadas que se pretenden mitigar, 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.

Subsistemas de riesgos

La entidad cuenta con un Manual del Sistema Integrado de Gestión del Riesgo - SIGR y el mapa de riegos institucional, en el cual se identifican los subsistemas de administración de riesgo y como entre sí se articulan, para este caso tenemos al subsistema seguridad de la información articulado al riesgo actuarial.

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.

Efectos

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, Perdidas económicas, Perjuicio de la imagen, Sanciones legales, reproceso, Demoras, Insatisfacción, entre otras.

Calidad de los controles

Se describen los controles implementados o barreras que existen actualmente para evitar la materialización del riesgo, se pueden encontrar actividades que desde la oficina de sistemas y el profesional universitario de sistemas se pueda adelantar.

Dentro del mapa de riesgos institucional se evidencia el mapa de calor para la evaluación del riesgo.

Tratamiento y seguimiento del Riesgo:

Se describen las opciones de manejo, plan de acción, soportes, responsables, con fechas de inicio y fin de las actividades. Las acciones propuestas pueden en algunos casos significar actualización de protocolos o procedimientos documentados, adopción de mejores prácticas a través de referenciaciones realizadas, fortalecimiento de buenas prácticas de, 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.

Para el tratamiento, seguimiento y control del riesgo, la entidad cuenta con un mapa de riesgos institucional.

6. CRONOGRAMA ACTIVIDADES

METAS/ACTIVIDADES	ENTREGABLE	CUMPLIMIENTO	PERIODO DE DESARROLLO	RESPONSABLE
Elaborar documento de responsabilidad para el acceso remoto a la red del hospital	Documento de responsabilidad individual de acceso remoto	100%	Primer semestre 2024	Profesional universitario de sistemas
Restructurar roles de acceso a la información de cada usuario en el sistema de información	Documento que evidencia o registros de los roles actualizados en el sistema de información Dinámica Gerencial	100%	Primer semestre 2024	Profesional universitario de sistemas
Socializar normatividad que rige la historia clínica digital al personal asistencial.	Listado de asistencia a la socialización, medido como talento humano asistente/talento humano convocado	100%	Toda la vigencia 2024	Profesional universitario de sistemas
Capacitación a usuarios internos y externos en riesgos de la información	Listado de asistencia de la capacitación, medido como talento humano asistente/talento humano convocado	100%	Toda la vigencia 2024	Profesional universitario de sistemas

7. CONTROL DE CAMBIOS

VERSIÓN	FECHA LIBERACIÓN DOCUMENTO			MOTIVO DEL CAMBIO
	DIA	MES	AÑO	
001	31	01	2023	Actualización de documento en contenido y normatividad vigente, se inicia versión toda vez que se incorpora en la nueva codificación del Sistema Integrado de Calidad de la institución.
002	31	01	2024	Actualización de documento, cambio de vigencia.

	ELABORÓ:	REVISÓ:	APROBÓ:
NOMBRE	**Miguel Ángel Rodríguez Herazo**	**William Humberto Salgado Gamboa**	**Duver Dicson Vargas Rojas**
CARGO	Profesional Universitario de sistemas	Subgerente Administrativo y Financiero	Agente Especial Interventor
FIRMA