Documentado.		Revisado	Aprobado
Nombre:	**HEYNER AROCA ARAÚJO**	**COMITÉ DE GESTIÓN Y DESEMPEÑO**	**MAGRETH SÁNCHEZ BLANCO**
Cargo:	**PROFESIONAL UNIVERSITARIO SISTEMAS**	**MIEMBROS COMITÉ**	**PRESIDENTE COMITÉ MIPG**
Firma:	**P/D: Original Firmado**	**Acta No 5 del 30 de Enero de 2019**	**P/D: Original Firmado**

1. INTRODUCCIÓN

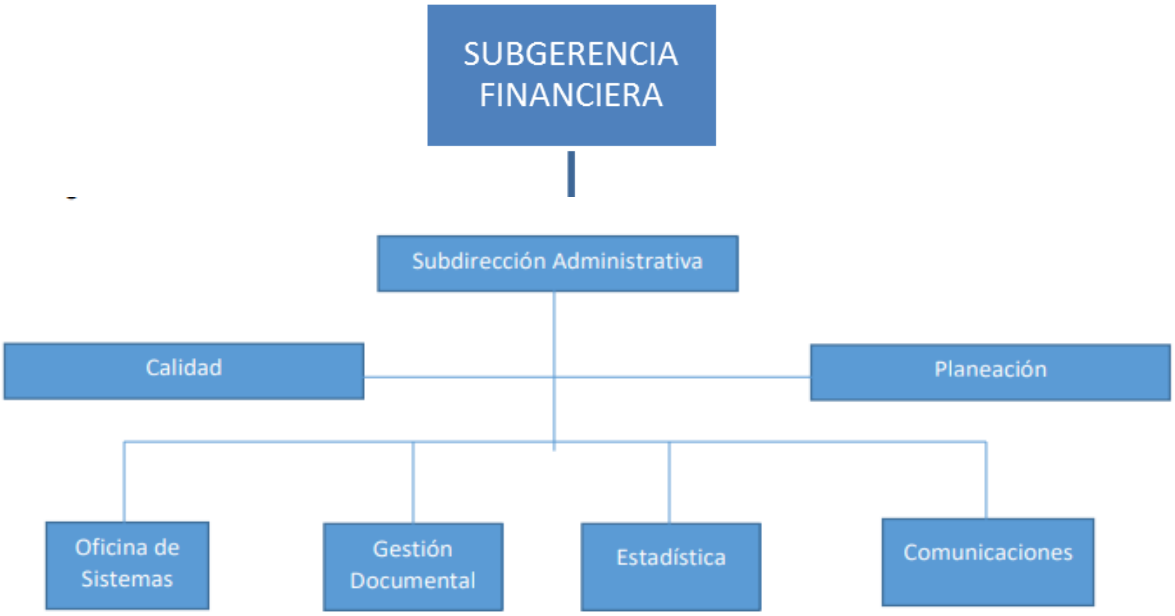
El plan de Riesgos de Seguridad y Privacidad aplica a todos los procesos de La **ESE Hospital Rosario Pumarejo de López**, los cuales manejen, procesen o interactúen con información institucional. La cual busca mejorar continuamente a través de la implementación de un método lógico y sistemático que permita identificar, analizar, evaluar, tratar, monitorear y comunicar los riesgos asociados al manejo de la información institucional, para lograr que estos no afecten de una manera relevante a la misma.

La institución en su quehacer diario utiliza TIC en cuanto a captura, procesamiento y reporte de información tanto internamente como externamente para comunicarse con los diferentes actores del sistema de salud, lo cual implica que la institución sea vulnerable a ataques mal intencionados o mala manipulación de la información lo que acarrea problemas económicos, legales, y administrativos por lo cual este documento busca establecer una línea de trabajo que permita a la entidad sortear los riesgos que lo rodean y lograr que su información este segura.

2. GENERALIDADES:

RESPONSABLES

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



- Subgerente Financiero
- Profesional Universitarios de Planeación
- Profesional Universitarios de Calidad
- Ingeniero de Sistemas
- Técnico en gestión documental
- Profesional Especializada Estadística
- SIAU

PLATAFORMA ESTRATEGICA.

Misión.

Somos una Empresa Social del Estado prestadora de servicios de salud de mediana complejidad en el Departamento del Cesar y áreas de influencia, por tener un talento humano idóneo, comprometida con la satisfacción de las necesidades del usuario, su familia, incluyente y participativa, fundamentada en la relación docencia servicio; respetuosa del entorno ambiental.

Visión.

Nuestro hospital en el año 2020 será una institución de alta complejidad, líder en la prestación de servicios de salud, aplicando altos estándares de calidad con humanización, en búsqueda permanente de la excelencia.

PRINCIPIOS Y VALORES:

Principios.

El Hospital en el desarrollo de las acciones en salud ha fundamentado los siguientes principios que soportan su cultura organizacional y son la base del sistema de valores éticos adoptados por los servidores públicos de la entidad.

- **HUMANIZACION:** Trato con calidez y dignidad.
- **PERTINENCIA:** Atención científica con el mínimo riesgo de acuerdo a la necesidad.
- **OPORTUNIDAD:** Garantizar los servicios requeridos sin retraso.
- **INTEGRALIDAD:** Cobertura de las necesidades de salud y satisfacción del usuario.
- **TRABAJO EN EQUIPO:** Cooperación y armonía para el logro de objetivos.

Valores.

Los valores éticos se presentan y establecen de manera explícita así como a través de un compromiso de la fuerza laboral para consolidad la cultura organizacional. De esta forma, la creación de las estrategias habilitan las capacidades organizacionales con los clientes externos e internos a ella bajo la concepción de una filosofía de integralidad para mantener la identidad mediante una proyección ética. Es decir, cuanto mejor sea la relación entre estas actividades y características administrativas, más probables será que haya una ejecución estratégica visible para alcanzar un beneficio rentable. Pelekais y Caridad (2013), gestión del talento humano.

Los Valores que rigen la forma de actuar de los servidores públicos en esta Institución se describen a continuación:

- **HONESTIDAD:** Este valor busca en los servidores del Hospital generar confianza y credibilidad en la sociedad a través de comportamientos y actitudes íntegras y transparentes.
- **RESPETO:** Se busca en los servidores del hospital valorar sus fortalezas, tolerar sus debilidades y aceptar su forma de pensar y actuar.

- **COMPROMISO:**

- **DILIGENCIA: cumplir con los deberes asignados funciones, responsabilidad con atención, prontitud y eficiencia para optimizar el uso de los recursos del estado.**

- **JUSTICIA: actuar con imparcialidad garantizando los derechos de las personas con equidad, igualdad y sin discriminación.**

- **SOLIDARIDAD:** Los servidores hospital desarrollan actitudes de fraternidad y ayuda mutua, promoviendo condiciones que permitan el crecimiento de las personas en todas las dimensiones posibles dentro de un ambiente de equidad y justicia social.

- **TOLERANCIA:** Este valor busca que los servidores del hospital actúen respetando y aceptando las diferencias que caracterizan a las personas.

3. GLOSARIO.

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.
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.

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.

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.

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.

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.

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.

Seguridad de la información: Preservación de la confidencialidad, integridad, y disponibilidad de la información.

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.

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.

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas.

Parte interesada: Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

4. 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.

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.
TE: 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 La ESE Hospital Rosario Pumarejo de López.

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, Perdidas 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.

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 común en circunstancias actuales
IMPACTO		
Muy bajo	1	Los efectos de materialización del riesgo no son significativos
Bajo	2	Los efectos de materialización del riesgo son poco significativos

Moderado	3	Los efectos de materialización del riesgo pueden significar aspectos
Alto	4	Los efectos de materialización del riesgo son significativos e importantes
Muy Alto	5	Los efectos son catastróficos, como muerte, lesiones incapacitantes o liquidación 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
		IMPACT				

NIVEL DE RIESGO	MEDIDAS DE
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
INACEPTABLE	EVITAR-COMPARTIR-TRANSFERIR POR MEDIO DE UN PLAN

Tratamiento y seguimiento del Riesgo:

Se describen los controles o barreras a ser implementadas que fortalezcan las existentes, 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 referenciaiones realizadas, 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.

CATEGORIA	Nº	IDENTIFICACION DE RIESGOS	FECHA DE IDENTIFICACION DE RIESGO	ANALISIS DEL RIESGO			VALORACION INICIAL DEL RIESGO			TRATAMIENTO Y SEGUIMIENTO DEL RIESGO						
				CAUSAS	CONSECUENCIAS	BARRERS DE SEGURIDAD EXISTENTES	VALOR DE PROBABILIDAD	VALOR DE IMPACTO	NIVEL DEL RIESGO	BARRERAS DE SEGURIDAD A IMPLEMENTAR	RESPONSABLE DEL SEGUIMIENTO	INDICADOR	LINEA BASE	META	RESULTADOS DE EFECTIVIDAD DE LAS ACCIONES (Planeación)	VALORACION DEL RIESGO DESPUES DE CONTROLES (Control Interno)

5. MARCO LEGAL.

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

Ley Estatutaria 1757 de 2015 - Promoción y protección del derecho a la participación democrática

Ley estatutaria 1618 de 2013: Ejercicio pleno de las personas con discapacidad

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

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

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