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

NIT. 890.204.895-0

LILIAM BEATRIZ SMITH SANCHEZ MURILLO
Gerente

VIGENCIA 2026

Km 1 Vía Puerto Berrio
Tels. (7) 6260141 / 6260330
Cimitarra, Santander
Nit. 890.204.895-0

Tabla de contenido

1. INTRODUCCIÓN

La información que genera constantemente la ESE Hospital Integrado San Juan de Cimitarra, Santander, 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 de 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 Integrado San Juan de Cimitarra, 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 Integrado San Juan de Cimitarra, 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. CONTEXTO ESTRATÉGICO:

2.1. MISIÓN

Prestar los servicios de salud de primer nivel, para toda la comunidad del área de influencia, de conformidad con los lineamientos establecidos por el sistema general de seguridad Social en Salud, cumplidores de los principios de eficiencia, eficacia, oportunidad, accesibilidad y calidad, en la prestación del servicio, contando con equipos y recurso humano debidamente capacitado y con un profundo sentido humano.

2.2. VISIÓN

Para el año 2030 seremos una institución de mayor nivel con infraestructura, dotación y con tecnología de última generación. Con un servicio humanizado en la atención segura al usuario y la familia. Serán la expresión de un sano equilibrio entre el balance social y económico lo que darán la solidez estructural necesaria para adaptarse a los cambios del medio.

2.3. POLITICA DE INTEGRIDAD

La ESE Hospital Integrado San Juan de Cimitarra, Santander consolida la integridad como principal prevención de la corrupción y motor del cambio de los comportamientos de los servidores públicos. Esta política se basa en la prevención de la corrupción, herramientas de seguimiento y control, y al establecimiento y promoción de valores, incentivar a los servidores públicos a interiorizar y fortalecer prácticas y comportamientos íntegros y ejemplares.

La ESE Hospital Integrado San Juan de Cimitarra, Santander consciente de la importancia de su función y de la responsabilidad que esta implica, con el propósito de garantizar el actuar y poniendo sobre manera los valores de HONESTIDAD, RESPETO, COMPROMISO, DILIGENCIA, JUSTICIA, ETICO Y PROFESIONAL del personal que lo conforma y de consolidar la confianza de la ciudadanía, implementa el Modelo de Integración de Planeación y Gestión orientado a promover y fortalecer la Integridad en el ejercicio de sus funciones.

3. OBJETIVOS

- ✓ Identificar y promover los valores y deberes íntegros promovidos por la ESE, que han de observar los servidores públicos en el desempeño de sus funciones.
- ✓ Establecer los criterios, conductas y controles que normen el comportamiento de los servidores públicos.
- ✓ Promover un ambiente de trabajo agradable y profesional, basado en el respeto, honestidad, compromiso, diligencia y justicia.
- ✓ Orientar la actuación de los servidores públicos.
- ✓ Consolidar la confianza de La ESE Hospital Integrado San Juan de Cimitarra, Santander, así como en el personal que la integra.

4. OBJETIVOS PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

4.1. Objetivo General

Vincular la identificación y análisis de Riesgos de la Entidad hacia los temas de la Seguridad de la Información con la Metodología de riesgos del DAFP.

La gestión de riesgos constituye una estrategia con el propósito de definir y aplicar los lineamientos para tratar de manera integral los riesgos de Seguridad Digital que La ESE Hospital Integrado San Juan de Cimitarra, pueda estar expuesto, y de esta manera alcanzar el plan estratégico, los objetivos, la misión y la visión institucional, protegiendo y preservando la integridad, confidencialidad y disponibilidad y de la información.

4.2. Objetivos de esta Gestión

- ✓ Cumplir con los requisitos legales y reglamentarios pertinentes a la legislación colombiana en materia de seguridad de la información.
- ✓ Gestionar riesgos de Seguridad y Privacidad de la información, Seguridad Digital, de acuerdo con los contextos establecidos en la Entidad.
- ✓ Fortalecer y apropiar conocimiento referente a la gestión de riesgos Seguridad y Privacidad de la información, Seguridad Digital.
- ✓ Alinear el Plan de Desarrollo Municipal, Plan de Desarrollo del Hospital General de Medellín y Plan de Seguridad y Privacidad de la ESE Hospital Integrado San Juan de Cimitarra, con este plan de tratamiento de riesgos.
- ✓ Emplear un enfoque de sistemas para planificar, implementar, monitorizar y gestionar los riesgos de seguridad digital.

5. ESTABLECER EL CONTEXTO PARA LA GESTIÓN DEL RIESGO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Corresponde a una visión general de los riesgos que pueden afectar el cumplimiento de los objetivos en este caso para la seguridad y privacidad de la información se analiza información de la estructura organizacional, del modelo de operación por procesos, del cumplimiento de planes y programas, de los recursos físicos y tecnológicos, entre otros. Para establecer el contexto para la gestión del riesgo es necesario definir los criterios de riesgo de seguridad y privacidad de la información:

5.1. CRITERIOS DE EVALUACIÓN DEL RIESGO:

Para la evaluación del riesgo con el fin de determinar el riesgo en la seguridad de la información de la ESE Hospital Integrado San Juan de Cimitarra, se tienen en cuenta los siguientes aspectos:

- ✓ El valor estratégico del proceso de información para la entidad
- ✓ La criticidad de los activos de información involucrados en el proceso
- ✓ Los requisitos legales y reglamentarios, así como las obligaciones contractuales
- ✓ La importancia de la disponibilidad de la, confidencialidad, e integridad de la información para las operaciones y la entidad.
- ✓ Las expectativas y percepciones de las partes interesadas y las consecuencias negativas para el buen nombre y la reputación de la entidad.

5.2. CRITERIOS DE IMPACTO.

Los criterios de impacto del riesgo se especifican en términos del grado de daño o de los costos para la entidad, causados por un evento de seguridad de la información, considerando los siguientes aspectos:

- ✓ Nivel de clasificación de los activos de información de los procesos
- ✓ Brechas en la seguridad de la información (ejemplo: perdidas de confidencialidad, integridad y disponibilidad de la información)
- ✓ Operaciones deterioradas
- ✓ Perdida del negocio y del valor financiero
- ✓ Alteración de planes y fechas limites
- ✓ Daños para la reputación
- ✓ Incumplimiento de los requisitos legales.

5.3. CRITERIOS DE ACEPTACIÓN DEL RIESGO

Los criterios de aceptación del riesgo pueden diferir de acuerdo con la expectativa de duración que se tenga del riesgo y se podrían considerar los siguientes elementos:

- ✓ Criterios del negocio
- ✓ Aspectos legales y reglamentarios
- ✓ Operaciones
- ✓ Tecnología
- ✓ Finanzas
- ✓ Factores sociales y humanitarios

La ESE Hospital Integrado San Juan de Cimitarra, cuenta con los siguientes criterios:

El riesgo inherente es importante porque la diferencia entre este y el riesgo residual proporciona una medida de la necesidad y la eficacia del tratamiento del riesgo actual. Si la diferencia entre el riesgo inherente y el residual es pequeña, el riesgo no necesita ser tratado o el tratamiento es ineficaz.
Para calcular el riesgo residual es necesario primero evaluar la efectividad de los controles.
Los responsables de los procesos, son los propietarios de sus riesgos y les corresponde rendir cuentas sobre su gestión, ellos deben realizar la medición de sus controles en términos de eficiencia, eficacia y efectividad para determinar la pertinencia, la necesidad de ajuste o modificación en caso de presentarse.

Cuando el impacto de la materialización del riesgo residual sea mayor o catastrófico, los responsables de los procesos y proyectos deben establecer planes de contingencia que permitan proteger la institución en caso de su ocurrencia.

Los procesos en los que se hayan identificado riesgos que no posean controles, deben diseñarse los mismos para evitar la materialización del riesgo o establecer acciones preventivas para eliminar la causa del posible riesgo.

5.4. TERMINOS Y 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 Agencia.

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

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.

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. 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.

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 con trol o las diferentes auditorías de los sistemas integrados de gestión.

Propietario del riesgo: Persona o entidad con la responsabilidad de rendir cuentas y la autoridad para gestionar un riesgo. Proceso: Conjunto de actividades interrelacionadas o que interactúan para transformar una entrada en salida.

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.

Riesgo: Efecto de la incertidumbre sobre los objetivos. 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.

Reducción del riesgo. Acciones que se toman para disminuir la probabilidad las consecuencias negativas, o ambas, asociadas con un riesgo.

Retención del riesgo. Aceptación de la pérdida o ganancia proveniente de un riesgo particular

Seguimiento: Mesa de trabajo semestral, en el cual se revisa el cumplimiento del plan de acción, indicadores y metas de riesgo y se valida la aplicación n de los controles de seguridad de la información sobre cada uno de los procesos.

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

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

MSPI: Modelo de Seguridad y privacidad.

Riesgos de seguridad digital: posibilidad de combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales. Incluye aspectos relacionados con el ambiente físico, digital y las personas.

6. POLÍTICA DE ADMINISTRACION DE RIESGOS

La ESE Hospital Integrado San Juan de Cimitarra, 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 la ESE Hospital Integrado San Juan de Cimitarra.

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

- ✓ *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, derivados financieros.

7. 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:

7.1. 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.

7.2. 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 acabo con un nivel adecuado de detalle que proporcione información suficiente para la valoración del riesgo.

7.3. 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) 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.

7.4. 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.

7.5. 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.

7.6. IDENTIFICACIÓN DE LAS CONSECUENCIAS

Para la identificación de las consecuencias es necesario tener:

- ✓ Lista de activos de información y su relación con cada proceso de la entidad.
- ✓ Lista de las amenazas y vulnerabilidades con respecto a los activos y su pertinencia.

NOTA: Una consecuencia puede ser la pérdida de la eficacia, condiciones adversas de operación, pérdida del negocio, reputación, daño, entre otros. Se deben identificar las consecuencias operativas de los escenarios de incidentes en términos de:

- ✓ Tiempo de investigación y reparación
- ✓ Pérdida de tiempo operacional
- ✓ Pérdida de oportunidad
- ✓ Salud y seguridad
- ✓ Costo financiero
- ✓ Imagen, reputación y buen nombre.

8. ANÁLISIS DE RIESGOS

Determinar las consecuencias o efectos de la posible ocurrencia del riesgo teniendo en cuenta los objetivos de la ESE Hospital Integrado San Juan de Cimitarra, las consecuencias pueden darse en personas, bienes materiales o intangibles como la imagen y prestigio corporativo. Para realizar el análisis se utiliza las siguientes tablas para evaluar la probabilidad y el impacto

Criterios para clasificar la probabilidad de ocurrencia del riesgo

Calificación		Variable
1	Remota	Improbable que ocurra
2	Rara	Posible que ocurra en algún momento
3	Ocasional	Probablemente ocurrirá
4	Frecuente	Probablemente ocurrirá en la mayoría de las circunstancias
5	Casi seguro	Se espera que el evento ocurra en la mayoría de las circunstancias

Criterios para la calificación del impacto del riesgo

Calificación		Variable
1	Insignificante	Las consecuencias de los riesgos, si ocurren no afectan a ningún proceso del Hospital.
2	Menor	Las consecuencias de los riesgos, si ocurren, afectan levemente al Hospital y pueden pasar desapercibidas para el paciente y no afectan la prestación del servicio ni la imagen institucional.
3	Moderado	Las consecuencias de los riesgos pueden afectar parcialmente los procesos y servicios del Hospital, pero las pérdidas y daños son menores y no afectan la imagen institucional.
4	Mayor	Las consecuencias de los riesgos pueden afectar de manera importante los procesos y servicios del Hospital y afectarse igualmente la imagen institucional.
5	Catastrófico	Las consecuencias pueden afectar totalmente al Hospital produciendo daños irrecuperables y afectarse la imagen institucional de manera grave.

8.1. EVALUACIÓN DE RIESGOS

Esta última etapa es la valoración del riesgo y se realiza de manera tal que permita establecer la probabilidad de su ocurrencia y el impacto sobre la operación del hospital. Para facilitar la calificación y evaluación a los riesgos, a continuación, se presenta una matriz que contempla un análisis cualitativo, para presentar la magnitud de las consecuencias potenciales (impacto) y la posibilidad de ocurrencia (probabilidad).

Criterios para la evaluación del riesgo Las categorías relacionadas con el Impacto son: insignificante, menor, moderado, alto y catastrófico. Las categorías relacionadas con la Probabilidad son: remota, raro, ocasional, frecuente, casi seguro

Probabilidad					
Casi seguro (5)					
Frecuente (4)					
Ocasional (3)					
Raro (2)					
Remota (1)					
	Insignificante (1)	Menor (2)	Moderado (3)	Alto (4)	Catastrófico (5)
Impacto					

8.2. TRATAMIENTO DE RIESGOS

Para el manejo de los riesgos se deben analizar las posibles acciones a emprender, las cuales deben ser factibles y efectivas, tales como: la implementación de las políticas, definición de estándares, optimización de procesos y procedimientos y cambios físicos entre otros. El tratamiento de riesgos implica tomar decisiones basadas en los resultados de la identificación de riesgos y su análisis. La política de gestión de riesgos está determinada por las siguientes opciones de tratamiento

Calificación		Tratamiento
Zona de Riesgo Bajo	Dada su baja probabilidad de presentación, es posible asumir el riesgo, pero deben planearse acciones para reducirlo en caso que se presente.	Asumir el riesgo
Zona de Riesgo Moderada	Evaluada la probabilidad e impacto es posible asumir el riesgo, pero siempre acompañado de acciones para reducirlo y evitarlo en lo posible.	Asumir el riesgo, Reducir el riesgo
Zona de Riesgo Alta	En esta zona de riesgo alta debe siempre evitar, reducir, compartir o transferir el riesgo.	Reducir el riesgo, evitar, compartir o transferir
Zona de Riesgo Extrema	En esta zona de riesgo extrema debe siempre y de manera simultánea: evitarse el riesgo, reducirlo y compartir o transferir el riesgo. Los puntos de control deben ser más estrictos	Reducir el riesgo, evitar, compartir o transferir

La gestión del riesgo está alineada con el modelo de mejoramiento institucional y es una de las fuentes de mejora. Para el tratamiento de los riesgos se implementan planes de mejoramiento, especialmente en los casos que se identifican nuevos riesgos, cuando es necesario rediseñar los controles existentes o definir unos nuevos controles.

9. METODOLOGÍA

El Plan de Tratamiento de Riesgos contempla la definición de las actividades a desarrollar en aras de mitigar los riesgos sobre los activos de información de los diferentes procesos de la ESE Hospital Integrado San Juan de Cimitarra.

10. COMUNICACIÓN Y CONSULTA

La comunicación es muy importante porque permite que todas las partes interesadas emitan su propio juicio sobre los riesgos; es importante tener en cuenta que las percepciones variarán en cuanto a los valores, necesidades, suposiciones, conceptos y preocupaciones de los interesados.

11. MONITOREO Y REVISIÓN

El monitoreo es esencial para asegurar que las acciones se están llevando a cabo y evaluar la eficiencia en su implementación: En primera instancia el seguimiento se debe llevar a cabo por el responsable del proceso (Director, Jefe, Líder). Segundo momento de seguimiento por parte del Subgerente (Procesos asistenciales, procesos administrativos y financiero)

La Oficina de Control Interno comunicará y presentará luego del seguimiento y evaluación, los resultados y propuestas de mejoramiento y tratamiento a las situaciones detectadas Por lo menos cada semestre, cada responsable de proceso realizará una autoevaluación a la gestión del riesgo, determinando la efectividad de sus controles para minimizar el riesgo, a su vez la Oficina de Control Interno realizará su propio informe de evaluación de riesgos y controles de segundo orden.

12. MECANISMOS DE SEGUIMIENTO Y VERIFICACIÓN

Los atributos establecidos para valorar el desempeño de la gestión de riesgos es una parte de la evaluación global de la institución y de la medición del desempeño de las áreas y de las personas. Las valoraciones integrales de toda la institución y particulares por proceso, proyecto o estrategia correspondiente a la disminución del nivel de vulnerabilidad, por lo que se tiene el siguiente indicador: Índice de riesgo residual por proceso: Expresado como proporción o porcentaje de la reducción de los valores estimados de probabilidad e impacto, luego de aplicar las medidas de gestión de riesgos para cada proceso o proyecto.

LILIAM B. SANCHEZ MURILLO
Gerente
ESE. Hospital Integrado San Juan de Cimitarra

Proyecto ELIANA BENAVIDES GALEANO – Control Interno