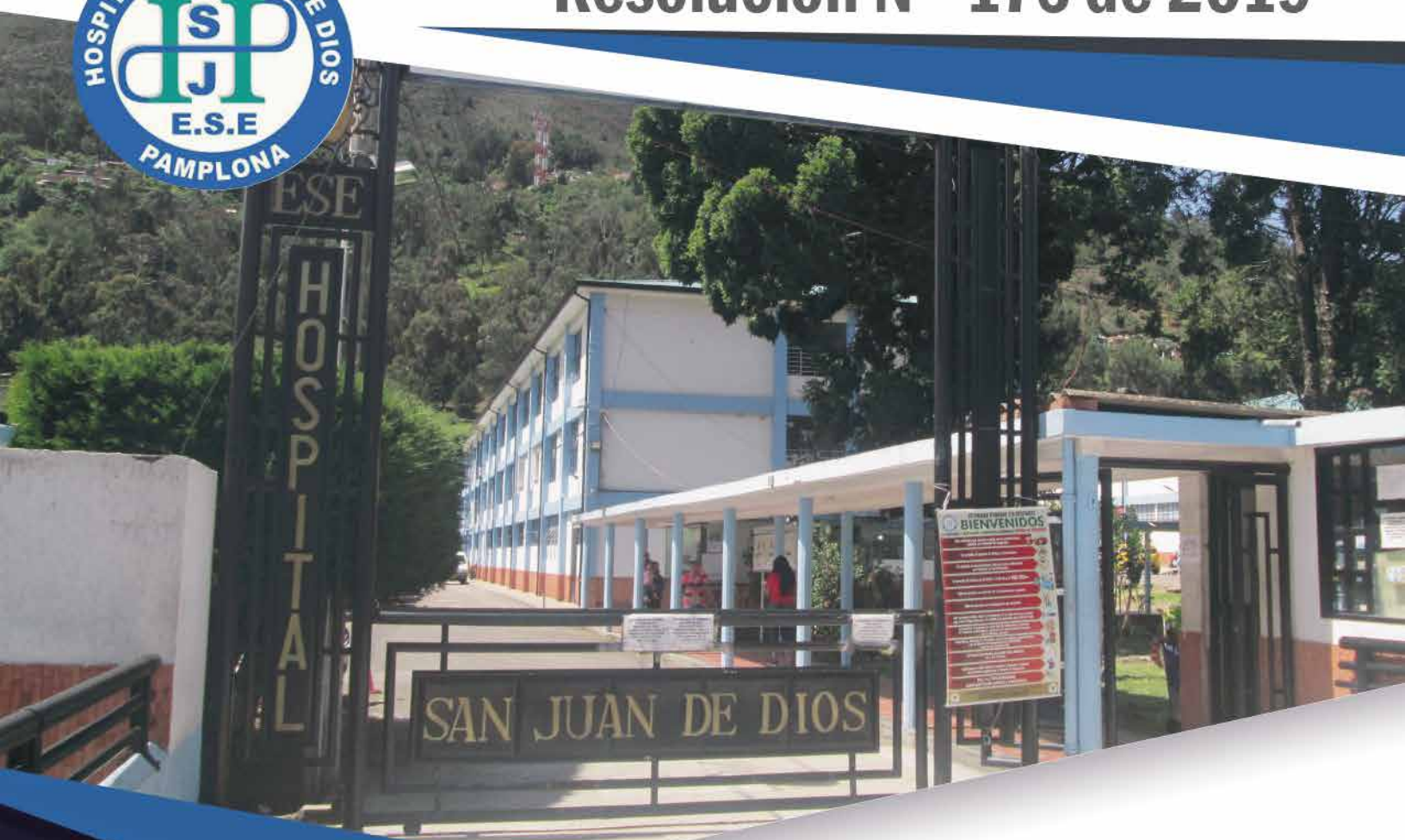
Resolución N° 176 de 2019



Política Administración del Riesgo

Política Administración del Riesgo

La Política de Administración del Riesgo de la ESE Hospital San Juan de Dios de Pamplona fue adoptada mediante resolución N° 176 del 13 de Junio de 2019.

La política hace parte integral de la metodología de Administración del Riesgo.

Presentación

La E.S.E Hospital San Juan de Dios de Pamplona en el marco de la implementación del Modelo Integrado de Planeación y Gestión—MIPG, Tomando como Herramienta para la consecución de los objetivos institucionales la administración del Riesgo, presenta su política de Administración del Riesgo de Gestión, Corrupción y Seguridad Digital, la cual establece acorde a las directrices impartidas por el Departamento Administrativo de la Función Pública—DAFP.

Objetivo

Establecer los lineamientos para el control y la gestión de todo tipo de riesgos a los que se encuentra expuesta la E.S.E Hospital san Juan de Dios de Pamplona, con el fin de minimizar su incidencia sobre la consecución de los objetivos estratégicos y de los procesos.

Alcance

La política de riesgos es aplicable a todos los procesos y proyectos de la Entidad y a todas acciones ejecutadas por los servidores durante el ejercicio de sus funciones.

Política General

La ESE Hospital San Juan de Dios de Pamplona, se compromete a administrar los riesgos de gestión, de corrupción y de seguridad de la información, inherentes a cada uno de sus procesos, estableciendo y ejecutando actividades de control, que le permitan a la entidad contrarrestar aquellos eventos que puedan afectar el logro de sus objetivos.

Metodología

Para la aplicación de la Administración del Riesgo en la entidad, se tendrán en cuenta la Guía para la Administración de Riesgo y el diseño de controles en entidades públicas, emitida por el Departamento Administrativo de la Función Pública y el procedimiento y formatos que a partir de la misma se establezcan en la entidad.

Tipos de Riesgos

De acuerdo con la naturaleza de la entidad, los objetivos institucionales y el ciclo de operación, se han identificado los siguientes tipos de riesgos:

Riesgo Estratégico: Probabilidad de acontecimientos que afecten los objetivos estratégicos de la organización pública y por tanto impactan toda la entidad.

Riesgos Gerenciales: Posibilidad de ocurrencia de eventos que afecten los procesos gerenciales y/o la alta dirección.

Riesgos de Imagen: Eventual realización de un evento que afecte la imagen, buen nombre o reputación de una organización ante sus clientes y partes interesadas.

Riesgos Operativos: Posibilidad de acontecimiento que afecten los procesos misionales de la entidad.
Riesgos Financieros: Posibilidad de ocurrencia de eventos que afecten los estados financieros y todas aquellas áreas involucradas con el proceso financiero como presupuesto. Tesorería, contabilidad, cartera, central de cuentas, costos , etc.

Riesgos de Cumplimiento: Posibilidad de ocurrencia de imprevistos que afecten la situación jurídica o contractual de la organización debido a su incumplimiento o desacato a la normatividad legal y las obligaciones contractuales.

Riesgos de Corrupción: Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.

Riesgos de Tecnología: Posibilidad de ocurrencia de hechos que afecten la totalidad o parte de la infraestructura tecnológica (hardware, software, redes, etc.) de una entidad.

Riesgos de Seguridad Digital: Posibilidad de combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas.

Criterios para Calificar el Impacto en Riesgos de Gestión

Los siguientes corresponden a los criterios que se tendrán en cuenta para determinar el impacto en riesgos de gestión.

Niveles para calificar el impacto	Impacto (consecuencias) Cuantitativo	Impacto (consecuencias) Cualitativo
CATASTRÓFICO	• Impacto que afecte la ejecución presupuestal en un valor ≥ 50% • Pérdida de cobertura en la prestación de los servicios de la entidad ≥ 50%. • Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor =50% • Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥ 50% del presupuesto general de la entidad.	• Interrupción de las operaciones de la Entidad por más de cinco (5) días. • Intervención por parte de un ente de control u otro ente regulador. • Pérdida de Información crítica para la entidad que no se puede recuperar. • Incumplimiento en las metas y objetivos institucionales afectando de forma grave la ejecución presupuestal. • Imagen institucional afectada en el orden nacional o regional por actos o hechos de corrupción comprobados.
MAYOR	• Impacto que afecte la ejecución presupuestal en un valor ≥ 20% • Pérdida de cobertura en la prestación de los servicios de la entidad ≥ 20%. • Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥ 20% • Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥ 20% del presupuesto general de la entidad.	• Interrupción de las operaciones de la Entidad por más de dos (2) días. • Pérdida de información crítica que puede ser recuperada de forma parcial o incompleta. • Sanción por parte del ente de control u otro ente regulador. • Incumplimiento en las metas y objetivos institucionales afectando el cumplimiento en las metas de gobierno. • Imagen institucional afectada en el orden nacional o regional por incumplimientos en la prestación del servicio a los usuarios o ciudadanos

MODERADO	• Impacto que afecte la ejecución presupuestal en un valor ≥ 5% • Pérdida de cobertura en la prestación de los servicios de la entidad ≥10%. • Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥ 5% • Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥ 5% del presupuesto general de la entidad.	• Interrupción de las operaciones de la Entidad por un (1) día. • Reclamaciones o quejas de los usuarios que podrían implicar una denuncia ante los entes reguladores o una demanda de largo alcance para la entidad. • Imagen institucional afectada en el orden nacional o regional por retrasos en la prestación del servicio a los usuarios o ciudadanos. • Investigaciones penales, fiscales o disciplinarias.
MENOR	• Impacto que afecte la ejecución presupuestal en un valor ≥ 1% • Pérdida de cobertura en la prestación de los servicios de la entidad ≥ 5%. • Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥ 1% • Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥ 1% del presupuesto general de la entidad.	• Interrupción de las operaciones de la Entidad por algunas horas. • Reclamaciones o quejas de los usuarios que implican investigaciones internas disciplinarias. • Imagen institucional afectada localmente por retrasos en la prestación del servicio a los usuarios o ciudadanos.
INSIGNIFICANTE	• Impacto que afecte la ejecución presupuestal en un valor ≥ 0,5% • Pérdida de cobertura en la prestación de los servicios de la entidad ≥ 1%. • Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥ 0,5% • Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥ 0,5%del presupuesto general de la entidad.	• No hay interrupción de las operaciones de la entidad. • No se generan sanciones económicas o administrativas. • No se afecta la imagen institucional de forma significativa.

CRITERIOS PARA CALIFICAR EL IMPACTO EN RIESGOS DE CORRUPCION

Los siguientes corresponden a los criterios que se tendrán en cuenta para determinar el impacto en riesgos de corrupción.

N°	Pregunta	Respuesta	
	Si el riesgo de corrupción se materializa podría...	SI	NO
1	¿Afectar al grupo de funcionarios del proceso?		
2	¿Afectar el cumplimiento de metas y objetivos de la dependencia?		
3	¿Afectar el cumplimiento de misión de la Entidad?		
4	¿Afectar el cumplimiento de la misión del sector al que pertenece la Entidad?		
5	¿Generar pérdida de confianza de la Entidad, afectando su reputación?		
6	¿Generar pérdida de recursos económicos?		
7	¿Afectar la generación de los productos o la prestación de servicios?		
8	¿Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien o servicios o los recursos públicos?		
9	¿Generar pérdida de información de la Entidad?		
10	¿Generar intervención de los órganos de control, de la Fiscalía, u otro ente?		
11	¿Dar lugar a procesos sancionatorios?		
12	¿Dar lugar a procesos disciplinarios?		
13	¿Dar lugar a procesos fiscales?		
14	¿Dar lugar a procesos penales?		
15	¿Generar pérdida de credibilidad del sector?		
16	¿Ocasionar lesiones físicas o pérdida de vidas humanas?		
17	¿Afectar la imagen regional?		
18	¿Afectar la imagen nacional?		
19	¿Generar daño ambiental?		
	TOTAL	**0**	**0**

- Responder afirmativamente de UNA a CINCO pregunta(s) genera un impacto Moderado.
- Responder afirmativamente de SEIS a ONCE preguntas genera un impacto Mayor.
- Responder afirmativamente de DOCE a DIECINUEVE preguntas genera un impacto Catastrófico.

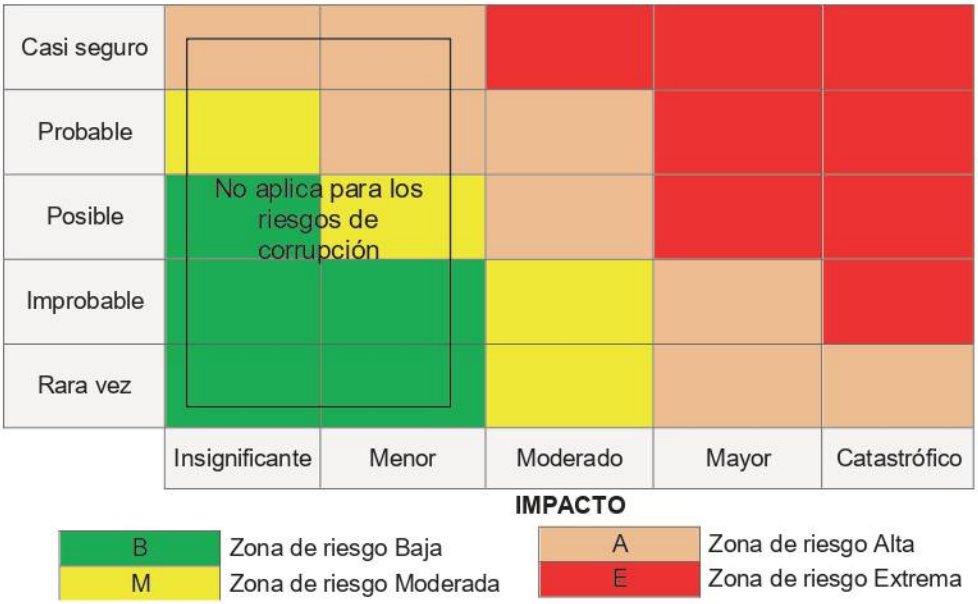
CRITERIOS PARA CALIFICAR EL IMPACTO EN RIESGOS DE SEGURIDAD DIGITAL

Los siguientes corresponden a los criterios que se tendrán en cuenta para determinar el impacto en riesgos de seguridad digital.

NIVEL	VALOR DEL IMPACTO	CRITERIOS DE IMPACTO PARA RIESGOS DE SEGURIDAD DIGITAL	
		IMPACTO (CONSECUENCIAS) CUANTITATIVO	IMPACTO (CONSECUENCIAS) CUALITATIVO
INSIGNIFICANTE	1	Afectación ≥1% de la población. Afectación ≥1% del presupuesto anual de la entidad.	Sin afectación de la integridad. Sin afectación de la disponibilidad. Sin afectación de la confidencialidad.
MENOR	2	Afectación ≥5% de la población. Afectación ≥5% del presupuesto anual de la entidad.	Afectación leve de la integridad. Afectación leve de la disponibilidad. Afectación leve de la confidencialidad.
MODERADO	3	Afectación ≥10% de la población. Afectación ≥10% del presupuesto anual de la entidad.	Afectación moderada de la integridad de la información debido al interés particular delos empleados y terceros. Afectación moderada de la disponibilidad de la información debido al interés particular de los empleados y terceros. Afectación moderada de la confidencialidad de la información debido al interés particular de los empleados y terceros.
MAYOR	4	Afectación ≥25% de la población. Afectación ≥25% del presupuesto anual de la entidad.	Afectación grave de la integridad de la información debido al interés particular de los empleados y terceros. Afectación grave de la disponibilidad de la información debido al interés particular delos empleados y terceros. Afectación grave de la confidencialidad de la información debido al interés particular delos empleados y terceros.
CATASTRÓFICO	5	Afectación ≥50% de la población. Afectación ≥50% del presupuesto anual de la entidad.	Afectación muy grave de la integridad de la información debido al interés particular de los empleados y terceros. Afectación muy grave de la disponibilidad de la información debido al interés particular de los empleados y terceros. Afectación muy grave de la confidencialidad de la información debido al interés particular de los empleados y terceros.

MAPA DE CALOR

A continuación se muestra el mapa de calor que se tendrá en cuenta para determinar la intersección entre la probabilidad y el impacto y con ello determinar el nivel de riesgo.



NIVEL DE ACEPTACIÓN DEL RIESGO

TIPO DE RIESGO	ZONA DE RIESGO	NIVEL DE ACEPTACIÓN
Riesgo de Gestión y Riesgo de Seguridad Digital	Baja	- Se acepta el riesgo, sin embargo el riesgo debe ser objeto de seguimiento continuo.
	Moderada	- Se reduce el riesgo implementando controles preventivos. - Se hace seguimiento bimensual.
	Alta y Extrema	- Se reduce el riesgo implementando controles preventivos. - Se evita le riesgo, cancelando la actividad o actividades que causan los riesgos. - Se comparte el riesgo, transfiriendo o compartiendo el mismo. - Se hace seguimiento mensual.
Riesgo de corrupción	Moderada, Alta y Extrema	- Ningún de riesgo de corrupción es aceptado. - Se reduce el riesgo implementando controles preventivos. - Se evita le riesgo, cancelando la actividad o actividades que causan los riesgos. - Se comparte el riesgo, transfiriendo o compartiendo el mismo. - Se hace seguimiento mensual

ACCIONES A EMPRENDER ANTE LA MATERIALIZACIÓN DE RIESGOS

TIPO DE RIESGO	RESPONSABLE	ACCIONES
Riesgo de corrupción	Oficina de Control Interno	– Convocar al Comité de Coordinación de Control Interno e informar sobre los hechos detectados, desde donde se tomarán las decisiones para iniciar la investigación de los hechos. – Dependiendo del alcance (normatividad asociada al hecho de corrupción materializado), realizar la denuncia ante el ente de control respectivo. – Facilitar el inicio de las acciones correspondientes con el líder del proceso, para revisar el mapa de riesgos y sus controles asociados. – Verificar que se tomaron las acciones y se actualizó el mapa de riesgos.
	Líder del proceso u otro(s) funcionario(s) que participa(n) o interactúa(n) con el proceso	– Informar a la Alta Dirección sobre el hecho encontrado. – De considerarlo necesario, realizar la denuncia ante el ente de control respectivo – Iniciar con las acciones de contingencia necesarias. – Realizar el análisis de causas y determinar acciones preventivas y de mejora. – Análisis y actualización del mapa de riesgos.
Riesgo de Gestión y de Seguridad Digital (Zona de riesgo Extrema, Alta y Moderada)	Oficina de Control Interno	– Informar al líder del proceso sobre el hecho encontrado. – Orientar al líder del proceso para que realice la revisión, análisis y acciones correspondientes para resolver el hecho. – Verificar que se tomaron las acciones y que se actualizó el mapa de riesgos correspondiente. – Convocar al Comité de Coordinación de Control Interno e informar sobre la actualización realizada.
	Líder del proceso u otro(s) funcionario(s) que participa(n) o interactúa(n) con el proceso	– Tomar las acciones de contingencia necesarias, dependiendo del riesgo materializado. – Iniciar el análisis de causas y determinar acciones preventivas y de mejora. – Analizar y actualizar el mapa de riesgos. – Informar a la Alta Dirección sobre el hallazgo y las acciones tomadas.
Riesgo de Gestión y de Seguridad Digital (Zona de riesgo Baja)	Oficina de Control Interno	– Informar la líder del proceso sobre el hecho. – Orientar técnicamente sobre las acciones determinadas en la política de Riesgos institucional.
	Líder del proceso u otro(s) funcionario(s) que participa(n) o interactúa(n) con el proceso	– Iniciar el análisis de causas y determinar acciones preventivas y de mejora. – Analizar y actualizar el mapa de riesgos

ACCIONES DE CONTINGENCIA

Para los riesgos ubicados en Zonas de Riesgo moderada, alta y extrema, los responsables de los procesos deberán establecer acciones de contingencia, entendiéndose estas como las acciones se implementaran una vez un riesgo se materializa.

ROLES Y RESPONSABILIDADES

En la ESE Hospital San Juan de Dios son responsables de la Administración del riesgo las siguientes instancias:
NOTA: El cuadro se debe anexar como imagen por su extensión. Roles y Responsabilidades.

Línea de defensa	Responsables	Responsabilidades frente al riesgo
Estratégica	Alta dirección Comité de Control Interno	- Establece y aprueba la Política de Administración del Riesgo. - Analiza los cambios en el entorno tanto interno como externo, que puedan tener un impacto significativo en la operación de la entidad y que puedan generar cambios en la estructura de riesgos y controles. - Hace seguimiento a cada una de las etapas de la gestión del riesgo. - Realiza seguimiento y análisis periódico a los riesgos institucionales - Identifica posibles riesgos que se estén materializado. - Revisa periódicamente informes de riesgos que se han materializado. - Realimenta al Comité de Gestión y Desempeño sobre los ajustes que se deban hacer frente a la gestión del riesgo
Primera Línea	Gerentes Públicos	- Identifican y valoran los riesgos que pueden afectar el logro de los objetivos institucionales. - Definen y diseñan los controles a los riesgos. - A partir de la política de administración del riesgo, establecen sistemas de gestión de riesgos y las responsabilidades para controlar riesgos específicos bajo la supervisión de la alta dirección. Con base en esto, establecen los mapas de riesgos.

		- Identifican y controlan los riesgos relacionados con posibles actos de corrupción en el ejercicio de sus funciones y el cumplimiento de sus objetivos, así como en la prestación del servicio y/o relacionados con el logro de los objetivos. - Implementan procesos para identificar, disuadir y detectar fraudes; y revisan la exposición de la entidad al fraude con el auditor interno de la entidad
Segunda Línea	Líderes de Proceso	- Informan sobre la incidencia de los riesgos en el logro de objetivos y evalúan si la valoración del riesgo es la apropiada. - Aseguran que las evaluaciones de riesgo y control incluyan riesgos de fraude. - Monitorean cambios en el riesgo legal, regulatorio y de cumplimiento. - Consolidan los seguimientos a los mapas de riesgo. - Elaboran informes consolidados para las diversas partes interesadas. - Siguen los resultados de las acciones emprendidas para mitigar los riesgos, cuando haya lugar. - Los supervisores y/o interventores de contratos realizan seguimiento a los riesgos de estos e informan las alertas respectivas.
Tercera Línea	Oficina de Control Interno	- Asesorar en la metodología para la identificación y administración de los riesgos, en coordinación con la segunda línea de defensa. - Identificar y evaluar cambios que podrían tener un impacto significativo en el SCI, durante las evaluaciones periódicas de riesgos y en el curso del trabajo de auditoría interna. - Comunicar al Comité de Coordinación de Control Interno posibles cambios e impactos en la evaluación del riesgo, detectados en las auditorías. - Revisar la efectividad y la aplicación de controles, planes de contingencia y actividades de monitoreo vinculadas a riesgos claves de la entidad. - Alertar sobre la probabilidad de riesgo de fraude o corrupción en las áreas auditadas.

SOCIALIZACIÓN Y PUBLICACIÓN

La Política de Administración de Riesgos, el Mapa de Riesgos Institucional, los Mapas de Riesgos por procesos, se socializarán con el personal de la Entidad y será objeto de publicación en la página web institucional .

REVISION Y ACTUALIZACIÓN

Los Mapas de Riesgos por Proceso y el Mapa de Riesgos Institucional, serán objeto de revisión y actualización mínimo una vez al año, o cuando las circunstancias de los procesos y/o eventualidades institucionales así lo ameriten, a partir de cualquier hecho de carácter interno o externo que los afecte. Para tal resultado se tendrá en cuenta la metodología dispuesta por el Departamento Administrativo de la Función Pública y el procedimiento documentado al interior de la entidad

MONITOREO Y EVALUACION

Los lideres de proceso junto con su personal de apoyo llevaran a cabo monitoreo y evaluación permanente a la gestión de riesgos, de corrupción y de seguridad digital.

SEGUIMIENTO.

El seguimiento y evaluación a la implementación y efectividad de la Política de Administración del Riesgo y a la gestión del riesgo, estará a cargo del Comité de Coordinación del Sistema de Control Interno y se llevará a cabo como mínimo una vez al año.

El seguimiento a los mapas de riesgos está a cargo de la Oficina de Control interno, el cual se ejecutará de manera periódica y de los mismos se elaborarán los informes correspondientes que serán dados a conocer a la alta dirección.

El monitoreo a los riesgos de corrupción deberá ser objeto de publicación en la página web de la entidad y en un lugar de fácil acceso al ciudadano

HOSPITAL SAN JUAN DE DIOS

HSJP

E.S.E

PAMPLONA

“Juntos Construyendo un Servicio con Calidad Humana”

@esehospitalpamplona @HospPamplona www.hsdp.gov.co