POLÍTICA DE OPERACIÓN PARA LA ADMINISTRACIÓN DEL RIESGO EN EL HOSPITAL MILITAR CENTRAL

Aprobada mediante acta No. 06 de Comité Institucional de Gestión y Desempeño del 30 de Noviembre de 2020

TABLA DE CONTENIDO

1. INTRODUCCIÓN

El **Hospital Militar Central** en concordancia con el proceso de fortalecimiento organizacional determina la Administración del Riesgo como parte integral de la gestión de la entidad con el fin de favorecer el desarrollo, la sostenibilidad, el logro de los objetivos institucionales y dando cumplimiento a las directrices del Modelo Integrado de Planeación y Gestión – MIPG, al esquema de seguridad de las líneas de defensa definido en el Modelo Estándar de Control Interno – MECI, a la guía para la administración del riesgos del Departamento Administrativo de la Función Pública - DAFP, al Modelo de seguridad y privacidad de la información de la estrategia de Gobierno Digital y demás normatividad aplicable.

El presente documento establece lineamientos y parámetros necesarios para la identificación, análisis, valoración, evaluación, tratamiento y respuesta a los riesgos y escenarios de pérdida de continuidad de negocio que puedan afectar la misión, el cumplimiento de los objetivos estratégicos y la gestión de los procesos, proyectos y planes institucionales.

2. OBJETIVO

Establecer un marco de referencia general que involucre a todos los servidores públicos y contratistas del **HOSPITAL MILITAR CENTRAL** para la adecuada gestión del riesgo, por medio de la identificación de acciones de control, respuestas oportunas y estrategias institucionales frente a las diferentes situaciones que puedan afectar el cumplimiento de la misionalidad y el logro de los objetivos institucionales.

3. ALCANCE

La política de operación para la administración de riesgos es aplicable a todas las dependencias, procesos, proyectos y planes institucionales, con el fin de identificar, analizar, valorar, monitorear y dar tratamiento a los riesgos identificados durante el desarrollo de la gestión planificada y a todos los servidores públicos y contratistas en el ejercicio de sus funciones y obligaciones.

4. MARCO LEGAL

A continuación, se relaciona la normativa interna y externa la cual regirá el documento, de acuerdo a la siguiente tabla:

Tipo	Número	Fecha de expedición	Origen	Organismo emisor	Descripción
Ley	87	1993	Externo	Congreso de la República	Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del estado y se dictan otras disposiciones.
Ley	1474	2011	Externo	Congreso de la República	Artículo 73. Cada entidad del orden nacional, departamental y municipal deberá elaborar anualmente una estrategia de lucha contra la corrupción y de atención al ciudadano. Dicha estrategia contemplará, entre otras cosas, el mapa de riesgos de corrupción en la respectiva entidad, las medidas concretas para mitigar esos riesgos… Parágrafo. En aquellas entidades donde se tenga implementado un sistema integral de administración de riesgos, se podrá validar la metodología de este sistema con la definida por el Programa Presidencial de Modernización, Eficiencia, Transparencia y Lucha contra la Corrupción.”
Decreto	1083	2015	Externo	Departamento Administrativo de la Función Pública.	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública.
Decreto	124	2016	Externo	Departamento Administrativo de la Presidencia de la República	Por el cual se sustituye el Título 4 de la Parte 1 del Libro 2 del Decreto 1081 de 2015, relativo al "Plan Anticorrupción y de Atención al Ciudadano".

Tipo	Número	Fecha de expedición	Origen	Organismo emisor	Descripción
Decreto	1499	2017	Externo	Departamento Administrativo de la Función Pública.	Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015
NTC - ISO	31000	2018	Externo	Incontec	Gestión del Riesgo
Guía	Versión 4	2018	Externo	Departamento Administrativo de la Función Pública.	Guía para la administración del riesgo y el diseño de controles en entidades públicas

5. GLOSARIO

- **Administración del riesgo:** Actividades encaminadas a la intervención de los riesgos de la entidad, a través de la identificación, valoración, evaluación, manejo y monitoreo de los mismos de forma que se apoye el cumplimiento de los objetivos institucionales.
- **Amenazas:** Situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.
- **Análisis de Riesgos:** Determinación del impacto en función de la consecuencia o efecto y de la probabilidad de ocurrencia del riesgo.
- **Apetito del Riesgo:** Nivel de riesgo que la entidad puede aceptar, relacionado con sus objetivos, el marco legal y las disposiciones de la Alta Dirección y del Órgano de Gobierno. El apetito del riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.
- **CICCI:** Comité Institucional de Coordinación de Control Interno.
- **CGDI:** Comité de Gestión y Desempeño Institucional.
- **Consecuencia:** Los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.
- **Contingencia:** Posible evento futuro, condición o eventualidad.
- **Continuidad:** Capacidad de una organización para continuar la entrega de productos o servicios a niveles aceptables después de una crisis.
- **Corrupción:** Uso del poder para desviar la gestión de lo público hacia el beneficio privado. Causas: Medios, circunstancias, situaciones o agentes generadores del evento.
- **Control:** Acciones encaminadas a reducir la probabilidad de ocurrencia o el impacto que pueda generar la materialización del riesgo.
- **Crisis (Emergencia):** Ocurrencia o evento repentino, urgente, generalmente inesperado que requiere acción inmediata.
- **DAFP:** Departamento Administrativo de la Función Pública.
- **Establecimiento del Contexto:** Definición de los parámetros internos y externos que se han de tomar en consideración cuando se gestiona el riesgo.
- **Evento:** Hecho que se genera durante la gestión de un proceso afectando el logro del objetivo del mismo, tiene relación directa con las actividades críticas, las actividades de ruta crítica de los proyectos de inversión y las actividades críticas de control de los procesos.
- **Factibilidad:** Presencia de factores internos y externos que pueden propiciar el riesgo.
- **Frecuencia:** Periodicidad con que ha ocurrido un evento.

- **Gestión del riesgo:** Proceso efectuado para proporcionar un aseguramiento razonable con respecto al logro de los objetivos institucionales.
- **Identificación del Riesgo**: Descripción de la situación no deseada.
- **Impacto:** Se entiende como las consecuencias que puede ocasionar a la organización la materialización del riesgo.
- **Líneas de Defensa:** Proporciona una manera simple y efectiva para mejorar las comunicaciones en la gestión de riesgos y control mediante la aclaración de las funciones y deberes esenciales relacionados.
- **Mapa de Riesgos:** Documento que resume los resultados de las actividades de gestión del riesgo.
- **MIPG:** Modelo Integrado de Planeación y Gestión.
- **MECI:** Modelo Estándar de Control Interno.
- **Monitoreo:** Verificación, supervisión, observación crítica o determinación continua del estado con el fin de identificar cambios con respecto al nivel de desempeño exigido o esperado.
- **OAPL:** Oficina Asesora de Planeación.
- **OCIN:** Oficina de Control Interno.
- **Política de Riesgo:** Declaración de la dirección y las intenciones generales de una organización con respecto a la gestión del riesgo.
- **Probabilidad:** Se entiende como la posibilidad de ocurrencia del riesgo. Esta puede ser medida con criterios de frecuencia o factibilidad.
- **Riesgo:** Efecto de la incertidumbre sobre los objetivos.
  (Nota: Un efecto es una desviación de aquello que se espera, sea positivo o negativo o ambos)
- **Riesgo de gestión:** Posibilidad de que suceda algún evento que tendrá un impacto sobre el cumplimiento de los objetivos institucionales. Se expresa en términos de probabilidad y consecuencias.
- **Riesgo Inherente:** Es aquel al que se enfrenta una entidad en ausencia de acciones de la dirección para modificar su probabilidad o impacto.
- **Riesgo residual:** Nivel de riesgo que permanece luego de tomar sus correspondientes medidas de tratamiento.
- **Riesgo de seguridad digital:** Combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, así como 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.
- **SVE:** Suite Vision empresarial.
- **TIC:** Tecnologías de la Información y las Comunicaciones.
- **Tolerancia al riesgo:** Son los niveles aceptables de desviación relativa a la consecución de objetivos. Pueden medirse y a menudo resulta mejor, con las mismas unidades que los objetivos correspondientes. Para el riesgo de corrupción la tolerancia es inaceptable.
- **Tratamiento:** Opciones que determinan el tipo de acciones a implementar para administrar el riesgo.
- **Valoración:** Grado de exposición al riesgo con la clasificación de probabilidad e impacto aplicando los controles existentes.
- **Vulnerabilidad:** Representan la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.

6. RESPONSABILIDADES

La responsabilidad está definida mediante las líneas de defensa y en el Hospital Militar Central se acogen de acuerdo a la siguiente tabla:

LÍNEA DE DEFENSA	RESPONSABLE	RESPONSABILIDAD FRENTE AL RIESGO.
		• Definir y aprobar el marco general para la gestión del riesgo, la

Línea Estratégica	• Comité de Gestión y Desempeño Institucional. • Comité Institucional de Control Interno.	gestión de la continuidad del negocio y el control. • Analizar los riesgos, vulnerabilidades, amenazas y escenarios de pérdida de continuidad de negocio institucionales que pongan en peligro el cumplimiento de los objetivos estratégicos, planes institucionales, metas, compromisos de la entidad y capacidades para prestar servicios. • Definir y aprobar la política para la administración del riesgo. • Garantizar el cumplimiento de los planes de la entidad
Primera Línea	• A cargo de los gerentes públicos – Subdirectores y Jefes de Oficina. • Líderes de los procesos, programas y proyectos de la entidad. • Jefes de Unidad.	• Identificar, valorar, evaluar y actualizar cuando se requiera, los riesgos que pueden afectar los objetivos, programas, proyectos y planes asociados a su proceso. • Definir, adoptar, aplicar y hacer seguimiento a los controles para mitigar los riesgos identificados y proponer mejoras para su gestión. • Supervisar la ejecución de los controles aplicados por el equipo de trabajo en la gestión del día a día, detectar las deficiencias de los controles y determinar las acciones de mejora a que haya lugar. • Revisar de acuerdo con su competencia y alcance la documentación de continuidad de negocio. • Desarrollar ejercicios de autoevaluación para establecer la eficiencia, eficacia y efectividad de los controles seleccionados para el tratamiento de los riesgos identificados y los planes de preparación frente a la pérdida de continuidad de negocio. • Informar a la Oficina de Planeación (segunda línea) sobre los riesgos materializados en los objetivos, programas, proyectos y planes de los procesos a cargo. • Reportar en la Suite Vision Empresarial – SVE los avances y realizar el cargue de las evidencias de la gestión de los riesgos dentro de los plazos establecidos.
Segunda Línea	• Jefe Oficina Asesora de Planeación. • Área Gestión de Calidad	• Orientar a la primera línea de defensa para que identifique, valore, evalúe y gestione los riesgos y escenarios de pérdida de continuidad de negocio en los temas de su competencia. • Acompañar a los líderes de procesos en la identificación, análisis, valoración, evaluación del riesgo, la definición de controles y las estrategias de continuidad de negocio asociadas a los escenarios de continuidad de negocio bajo su responsabilidad y los temas a su cargo. • Asesorar a la línea estratégica en el análisis del contexto interno y externo, para la definición de la política de riesgo, el establecimiento de los niveles de impacto y el nivel de aceptación del riesgo residual. • Consolidar el mapa de riesgos institucional, riesgos de mayor criticidad frente al logro de los objetivos) y presentarlo para análisis y seguimiento ante el CGDI. • Acompañar, orientar y capacitar a los líderes de procesos en la identificación, análisis, valoración y evaluación del riesgo. • Supervisar en coordinación con los demás responsables de esta segunda línea de defensa, que la primera línea identifique,

		analice, valore, evalúe y realice el tratamiento de los riesgos, que se adopten los controles para la mitigación de los riesgos identificados y se apliquen las acciones pertinentes para reducir la probabilidad o impacto de los riesgos. • Monitorear los controles establecidos por la primera línea de defensa, acorde con la información suministrada por los líderes de procesos. • Evaluar que la gestión de los riesgos este acorde con la presente política de la entidad y que sean monitoreados por la primera línea de defensa. • Promover ejercicios de autoevaluación para establecer la eficiencia, eficacia y efectividad de los controles establecidos para el tratamiento de los riesgos identificados. • Orientar y hacer seguimiento a las pruebas del plan de continuidad de negocio. • Identificar cambios en el apetito del riesgo en la entidad, especialmente en aquellos riesgos ubicados en zona baja y presentarlos para su aprobación del CICCI. • Actualizar, según se requiera, los escenarios de riesgo y la documentación asociada al plan de continuidad de negocio bajo su responsabilidad. • Garantizar la publicación en la intranet de la versión actualizada del mapa de riesgos institucional - Área de Gestión de Calidad
Segunda Línea	• Jefes de Oficina. • Jefes de Unidad. • Jefes de Servicios. • Supervisores de Contrato	• Presentar el mapa de riesgos del proceso desarrollado en las mesas de trabajo a la primera línea para la aprobación y visto bueno. • Socializar y comunicar, al interior de sus procesos, la política de operación para la administración del riesgo, el mapa de riesgos y los resultados del seguimiento. • Monitorear los riesgos identificados y aplicar los controles definidos por la primera línea de defensa acorde con la estructura de los temas a su cargo. • Realizar el seguimiento al mapa de riesgos de su proceso. • Reportar en el módulo de riesgos del aplicativo SUITE VISION EMPRESARIAL el registro de los avances en la gestión del riesgo junto con las evidencias de aplicación de los controles. • Proponer las acciones de mejora a que haya lugar posterior al análisis, valoración, evaluación o tratamiento del riesgo. • Supervisar la implementación de las acciones de mejora o la adopción de buenas prácticas de gestión del riesgo asociado a su responsabilidad. • La Oficina Asesora Jurídica- OCIN, tendrá el compromiso de identificar, analizar, valorar y evaluar los riesgos y controles asociados a su gestión con enfoque en la prevención del daño antijurídico. • Comunicar al equipo de trabajo a su cargo la responsabilidad y resultados de la gestión del riesgo. • Comunicar oportunamente a la Oficina Asesora de Planeación y Oficina de Control Interno sobre la materialización de riesgos

		tipificados en cumplimiento del artículo 4º de la Ley 1150 de 2007 - supervisores de contrato.
Tercera línea	• Oficina de Control Interno	• Proporcionar aseguramiento objetivo sobre la eficacia de la gestión del riesgo y control, con énfasis en el diseño e idoneidad de los controles establecidos en los procesos. • Incluir el seguimiento al mapa de riesgo en el Plan Anual de Auditoria y reportar los resultados al CICCI. • Realizar el seguimiento a los riesgos y la medición del nivel de eficacia de los controles para el tratamiento de los riesgos identificados en las áreas en los diferentes niveles de operación de la entidad. • Realizar la verificación de las evidencias de la aplicación de los controles definidos en el mapa de riesgos institucional • Proporcionar aseguramiento objetivo en las áreas identificadas no cubiertas por la segunda línea de defensa. • Asesorar a la primera línea de defensa de forma coordinada con la Oficina de Planeación, en la identificación de los riesgos y diseño de controles. • Presentar al Comité Institucional de Coordinación de Control Interno el resultado de la medición del nivel de eficacia de los controles para el tratamiento de los riesgos identificados en las áreas en los diferentes niveles de operación de la entidad. • Recomendar mejoras a la política de operación para la administración del riesgo.

De igual manera, la *Oficina Asesora de Planeación* lleva a cabo las siguientes acciones durante el acompañamiento para la identificación y administración del riesgo:

- Comunicar a la entidad la política y el mapa de riesgos institucional y realizar las gestiones para su publicación en la página web de la entidad.
- Socializar a líderes de proceso la metodología de riesgos, los lineamientos de la primera línea de defensa frente al riesgo, objetivo del proceso, comunicación de los planes y proyectos del proceso asesorado.
- Capacitar al grupo de trabajo de cada dependencia para el reporte y cargue del mapa de riesgos y evidencias en la herramienta Suite Vision Empresarial –SVE.
- Liderar las mesas de trabajo de identificación del riesgo.
- Verificar que los controles estén definidos y se documenten conforme a los requerimientos de la metodología.
- Consolidar el mapa de riesgos institucional con la información presentada por los líderes de proceso, construida en las mesas de trabajo.
- Revisar que el cargue de información en la SVE esté acorde con lo aprobado.

Por su parte, *los líderes de proceso* tienen la responsabilidad de:

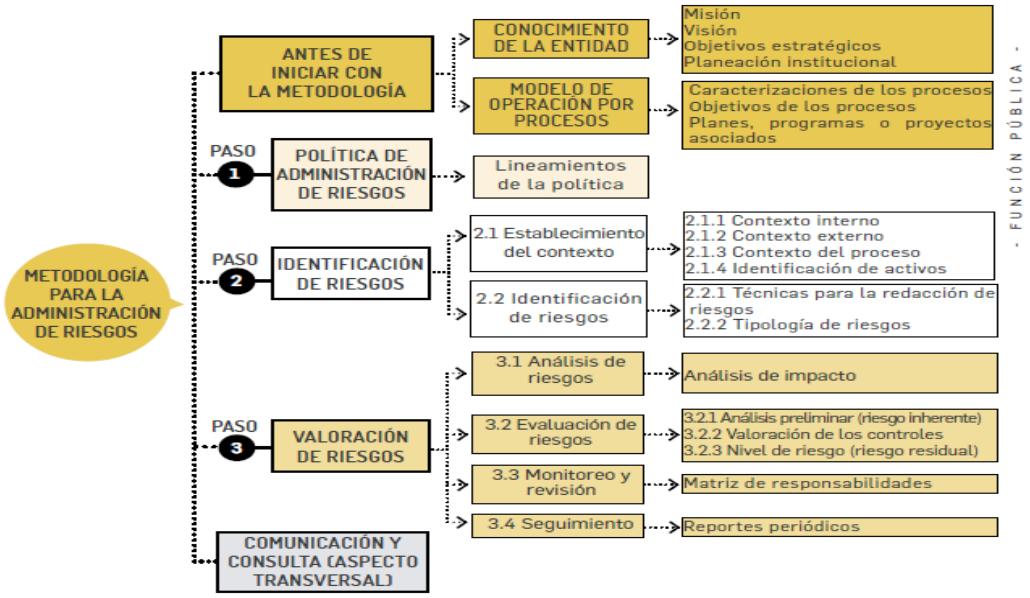
- Asegurar que al interior de su grupo de trabajo se reconozca el concepto de *"administración del riesgo"*, la política y la metodología definida, los actores y el entorno del proceso aprobados por la primera línea de defensa.

7. METODOLOGÍA

La metodología se fundamenta en la Guía para la administración del riesgo y el diseño de controles en entidades públicas versión 4, emitida por el Departamento Administrativo de la Función Pública y algunos elementos se adaptan de acuerdo con la estructura y características del Hospital Militar Central. Dicha metodología del DAFP establece tres (3) pasos básicos, los cuales son:

Política de Administración del Riesgo, Identificación del Riesgo y Valoración del Riesgo.

La gestión del riesgo facilita la toma de decisiones al interior de la organización, impulsando así el crecimiento y la sostenibilidad de las acciones adelantadas, por tal razón, a continuación se presenta la estructuración de la metodología de gestión del riesgo:



Fuente: *Guía para la administración del riesgo y el diseño de controles en entidades públicas v. 4 – Departamento Administrativo de la Función Pública.*

La metodología de administración del riesgo requiere un previo análisis y conocimiento de la entidad (Misión, Visión, objetivos estratégicos y planeación institucional), con el fin de establecer su complejidad, procesos, planeación institucional, permitiendo conocer y entender la Entidad y su entorno, lo que determinará el análisis de riesgos y la aplicación de la Metodología en general. Adicionalmente, se debe tener establecido y definido un modelo de operación por procesos, donde se tenga documentado mapa de procesos, caracterizaciones de procesos, objetivos de los procesos, planes, programas o proyectos asociados a cada proceso.

7.1. POLÍTICA DE ADMINISTRACIÓN DE RIESGOS

El Hospital Militar Central en ejercicio de su labor misional, se encuentra comprometido con la adecuada administración de los riesgos, para lo cual adelantará acciones de identificación, análisis, valoración, monitoreo y tratamiento de los riesgos que puedan afectar el logro de los objetivos institucionales.

7.2. IDENTIFICACIÓN DE RIESGOS

En esta fase se deben establecer las fuentes o factores de riesgo los eventos o riesgos, sus causas y consecuencias. Para el análisis se pueden involucrar datos históricos, análisis teóricos, opiniones informadas y expertas y las necesidades de las partes involucradas.

7.2.1. ESTABLECIMIENTO DEL CONTEXTO

En el ejercicio de identificación es necesario establecer el contexto tanto interno como externo de la entidad, además del contexto del proceso

7.2.1.1. ESTABLECIMIENTO DEL CONTEXTO INTERNO

En el contexto interno del Hospital Militar Central, identificado con base en la matriz FODA del Plan Estratégico Institucional 2019 – 2022, se consideran los factores que a continuación se relacionan:

FACTORES INTERNOS	DEFINICIÓN
Financieros	Presupuesto de funcionamiento, recursos de inversión, infraestructura, capacidad instalada.
Personal	Competencias del personal, disponibilidad del personal, seguridad y salud ocupacional.
Procesos	Capacidad, diseño, ejecución, proveedores, entradas, salidas, gestión del conocimiento.
Tecnología	Integridad de datos, disponibilidad de datos y sistemas, desarrollo, producción, mantenimiento de sistemas de información.
Estratégicos	Direccionamiento estratégico, planeación institucional, liderazgo, trabajo en equipo.
Comunicación Interna	Canales utilizados y su efectividad, flujo de la información necesaria para el desarrollo de las operaciones.

7.2.1.2. ESTABLECIMIENTO DEL CONTEXTO EXTERNO

En el contexto externo del Hospital Militar Central, identificado con base en la matriz FODA del Plan Estratégico Institucional 2019 – 2022, se consideran los factores que a continuación se relacionan:

FACTORES EXTERNOS	DEFINICIÓN
Políticos	Cambios de gobierno, legislación, políticas públicas, regulación.
Económicos y Financieros	Disponibilidad de capital, liquidez, mercados financieros, desempleo, competencia.
Sociales y Culturales	Demografía, responsabilidad social, terrorismo.
Tecnológicos	Avances en tecnología, acceso a sistemas de información externos, gobierno en línea.
Ambientales	Emisiones y residuos, energía, catástrofes naturales, desarrollo sostenible.

Legales y Reglamentarios	Normatividad externa (Leyes, decretos, ordenanzas y acuerdos).
Comunicación Externa	Mecanismos utilizados para entrar en contacto con los usuarios o ciudadanos, canales establecidos para que el mismo se comunique con la entidad.-

7.2.1.3. ESTABLECIMIENTO DEL CONTEXTO DEL PROCESO

La identificación del contexto del proceso se realiza a partir del conocimiento de situaciones o factores como:

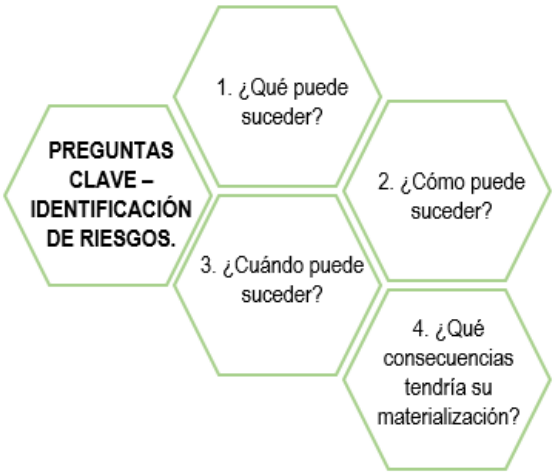
PROCESO	DEFINICIÓN
Diseño del proceso	Claridad en la descripción del alcance y objetivo del proceso.
Interacciones con otro procesos	Relación precisa con otros procesos en cuanto a insumos, proveedores, productos, usuarios o clientes.
Transversalidad	Procesos que determinan lineamientos necesarios para el desarrollo de todos los procesos de la entidad.
Procedimientos asociados	Pertinencia en los procedimientos que desarrollan los procesos.
Responsables del proceso	Grado de autoridad y responsabilidad de los funcionarios frente al proceso.
Comunicación entre los procesos	Efectividad en los flujos de información determinados en la interacción de los procesos.
Activos de Seguridad Digital del proceso	Información, aplicaciones, hardware entre otros, que se deben proteger para garantizar el funcionamiento interno de cada proceso, como de cara al ciudadano.

TÉCNICAS PARA LA IDENTIFICACIÓN DE RIESGOS

La identificación del riesgo se lleva a cabo determinando las causas con base en el contexto interno, externo y del proceso que pueden afectar el logro de los objetivos. Algunas causas externas no controlables por la entidad se podrán evidenciar en el análisis del contexto externo, para ser tenidas en cuenta en el análisis y valoración del riesgo.

A partir de este contexto se identifica el riesgo, el cual estará asociado a aquellos eventos o situaciones que pueden entorpecer el normal desarrollo de los objetivos del proceso o los estratégicos. El riesgo debe estar descrito de manera clara y precisa. Su redacción no debe dar lugar a ambigüedades o confusiones con la causa generadora de los mismos.

Las preguntas claves para la identificación del riesgo permiten determinar:

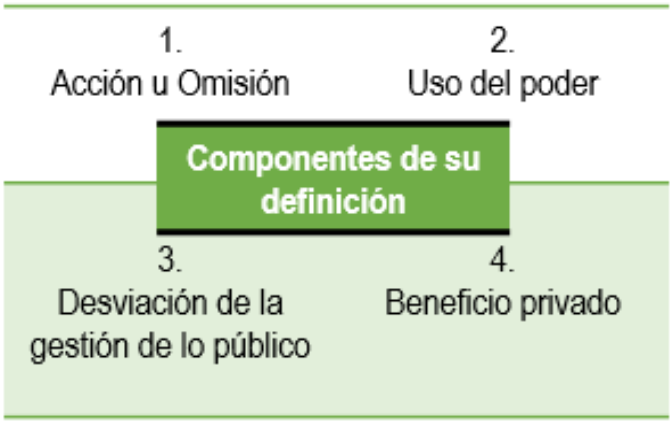


- **¿Qué puede suceder?** Identificar la afectación que puede darse en en el cumplimiento del objetivo estratégico o del proceso según sea el caso.
- **¿Cómo puede suceder?** Establecer las causas a partir de los factores determinados en el contexto.
- **¿Cuándo puede suceder?** Determinar de acuerdo con el desarrollo del proceso.
- **¿Qué consecuencias tendría su materialización?** Determinar los posibles efectos por la materialización del riesgo.

TÉCNICA DE IDENTIFICACIÓN DE RIESGOS DE CORRUPCIÓN

El riesgo de corrupción es la posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado. Los riesgos de corrupción se establecen sobre procesos.

"Esto implica que las prácticas corruptas son realizadas por actores públicos y/o privados con poder e incidencia en la toma de decisiones y la administración de los bienes públicos"
(Conpes N° 167 de 2013).



Es necesario que en la descripción del riesgo concurran los componentes de su definición, así:

ACCIÓN U OMISIÓN + USO DEL PODER + DESVIACIÓN DE LA GESTIÓN DE LO PÚBLICO + EL BENEFICIO PRIVADO.

Con el fin de facilitar la identificación de riesgos de corrupción y evitar que se presenten confusiones entre un riesgo de gestión y uno de corrupción, se ha diseñado la matriz de definición de riesgo de corrupción, que incorpora cada uno de los componentes de su definición.

De acuerdo con la matriz, si se marca con una (X) en la descripción del riesgo que aparece en cada casilla quiere decir que se trata de un riesgo de corrupción:

MATRIZ: DEFINICIÓN DEL RIESGO DE CORRUPCIÓN

Descripción del riesgo	Acción u Omisión	Uso del Poder	Desviar la gestión de lo público	Beneficio Privado
Posibilidad de recibir o solicitar cualquier dádiva o beneficio a nombre propio o de terceros con el fin de celebrar un contrato.	X	X	X	X

Una vez se identifiquen los riesgos de corrupción, estos deberán publicarse de manera que tanto servidores públicos, contratistas y la ciudadanía conozcan, debatan y formulen sus apreciaciones y propuestas sobre el proyecto del Mapa de Riesgos de Corrupción. En tal sentido se deberá dejar evidencia del proceso de socialización y publicarse sus resultados.

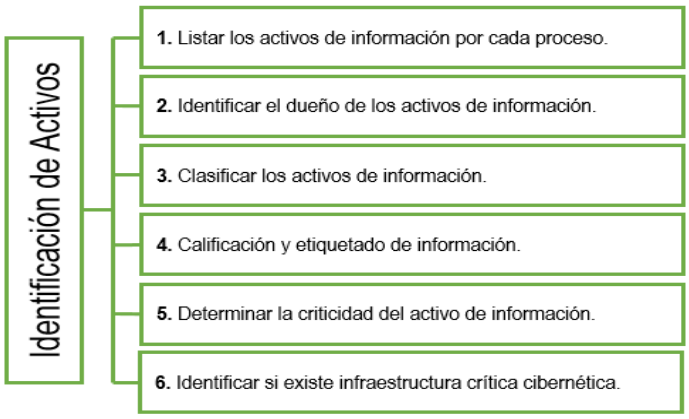
IDENTIFICACIÓN DE RIESGOS DE SEGURIDAD DIGITAL - ACTIVOS INFORMACIÒN

Los riesgos de seguridad digital se basan en la afectación de tres criterios en un activo de información o un grupo de activos de información dentro del proceso:

"Integridad, confidencialidad o disponibilidad"

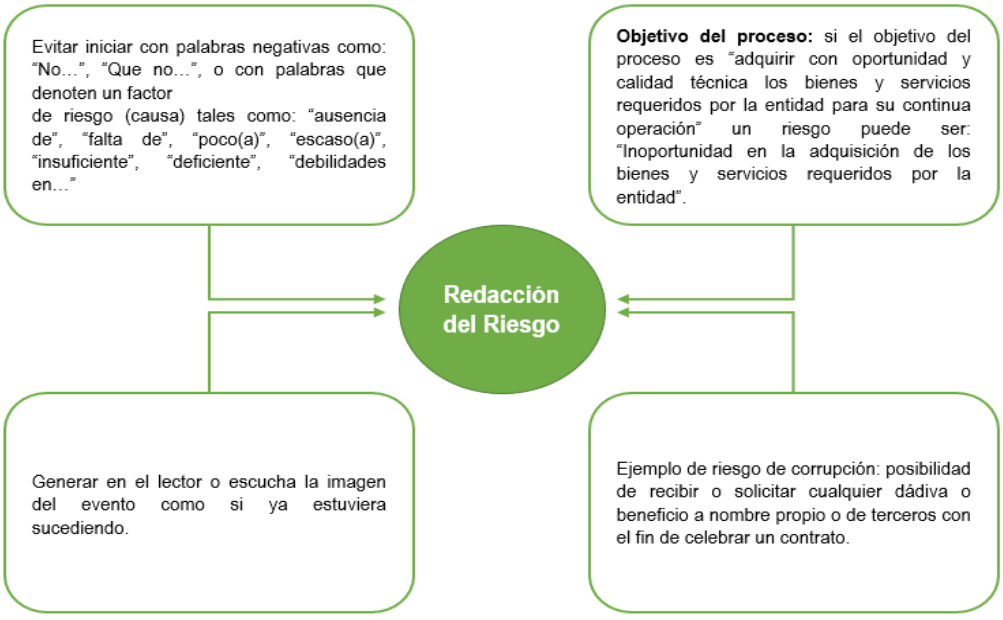
Existen tres (3) tipos de riesgos: Pérdida de confidencialidad, pérdida de la integridad y pérdida de la disponibilidad de los activos de información. Para cada tipo de riesgo se podrán seleccionar las amenazas y las vulnerabilidades que puedan causar que dicho riesgo se materialice.

Para el riesgo identificado se deben asociar el grupo de activos de información o activos de información específicos del proceso y, conjuntamente, analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización.



7.2.1.4. TÉCNICAS PARA LA REDACCIÓN DE RIESGOS

Redacción del riesgo:



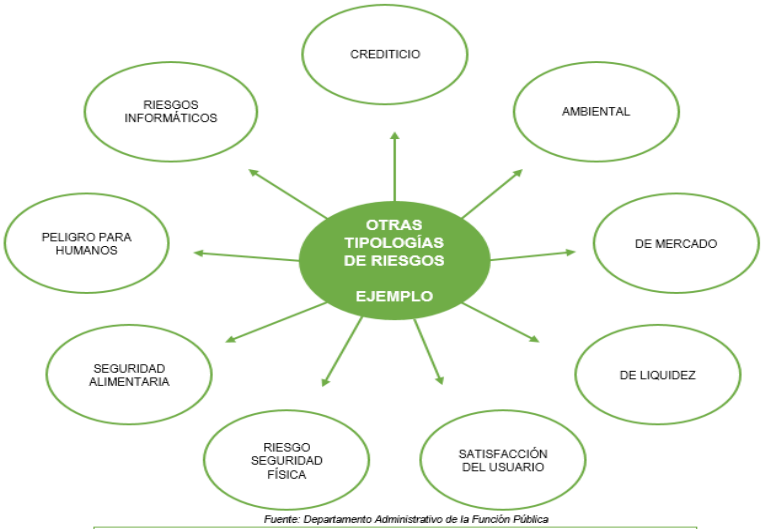
Fuente: Departamento Administrativo de la Función Pública

IMPORTANTE
Pregúntese si el riesgo de gestión identificado está relacionado directamente con las características del objetivo. Si la respuesta es "no", este puede ser la causa o la consecuencia.

7.2.1.5. TIPOLOGÍA DE RIESGOS

- **Riesgos estratégicos:** Posibilidad de ocurrencia de eventos que afecten los objetivos estratégicos de la organización pública y por tanto impactan toda la entidad.
- **Riesgos operativos:** Posibilidad de ocurrencia de eventos que afecten los procesos misionales de la entidad.
- **Riesgos gerenciales:** Posibilidad de ocurrencia de eventos que afecten los procesos gerenciales y/o la alta dirección.

- **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 tecnológicos:** Posibilidad de ocurrencia de eventos que afecten la totalidad o parte de la infraestructura tecnológica (hardware, software, redes, etc.) de una entidad.
- **Riesgos de cumplimiento:** Posibilidad de ocurrencia de eventos que afecten la situación jurídica o contractual de la organización debido a su incumplimiento o desacato a la normatividad legal y las obligaciones contractuales.
- **Riesgo de imagen o reputacional:** Posibilidad de ocurrencia de un evento que afecte la imagen, buen nombre o reputación de una organización ante sus clientes y partes interesadas.
- **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 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.



Fuente: Departamento Administrativo de la Función Pública

IMPORTANTE
La tipología de riesgos depende de la misión de cada entidad, de las normas que regulan su operación, de los sistemas de gestión que implemente, entre otros aspectos.
Los riesgos de corrupción, siempre deben gestionarse.

7.3. VALORACIÓN DE RIESGOS

En esta fase se establece la probabilidad de ocurrencia del riesgo y sus posibles efectos/consecuencias, con el fin de estimar la zona de riesgo inicial (riesgo inherente) y confrontar la efectividad de los controles establecidos que determinará la zona de riesgo final (riesgo residual).

NIVELES DE CALIFICACIÓN PROBABILIDAD E IMPACTO

En este punto se busca establecer la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto, con el fin de estimar la zona de riesgo inicial (RIESGO INHERENTE).

Aspectos a tener en cuenta:

- Criterios para determinar probabilidad.

- Criterios para determinar el impacto o consecuencias.
- Matriz de evaluación de riesgos.

7.3.1.1 PROBABILIDAD RIESGOS DE GESTIÓN, CORRUPCIÓN, SEGURIDAD DIGITAL

En esta fase del proceso se analiza qué tan posible es que ocurra el riesgo, se expresa en términos de frecuencia o factibilidad, donde frecuencia implica analizar el número de eventos en un periodo determinado, se trata de hechos que se han materializado o se cuenta con un historial de situaciones o eventos asociados al riesgo; factibilidad implica analizar la presencia de factores internos y externos que pueden propiciar el riesgo, se trata en este caso de un hecho que no se ha presentado pero es posible que suceda.

Criterios para calificar la Probabilidad			
Descriptor	**Descripción**	**Frecuencia**	**Nivel**
Rara vez	El evento puede ocurrir solo en circunstancias excepcionales (poco comunes o anormales).	No se ha presentado en los últimos 5 años.	1
Improbable	El evento puede ocurrir en algún momento.	Al menos 1 vez en los últimos 5 años.	2
Posible	El evento podrá ocurrir en algún momento.	Al menos 1 vez en los últimos 2 años	3
Probable	Es viable que el evento ocurra en la mayoría de las circunstancias	Al menos 1 vez en el último año.	4
Casi seguro	Se espera que el evento ocurra en la mayoría de las circunstancias	Más de 1 vez al año	5

7.3.1.1. IMPACTO RIESGOS DE GESTIÓN

Una vez identificada la probabilidad, se procede a realizar la calificación para establecer sus consecuencias o impacto, con el fin de estimar la zona de riesgo inicial (RIESGO INHERENTE). Para tal efecto se han definido las categorías que a continuación se presentan, con la respectiva descripción cuantitativa y cualitativa:

Medición Impacto Riesgos de Gestión			
Categoría	**Descripción Cuantitativa**	**Descripción Cualitativa**	**Nivel**
CATASTRÓFICO	* Impacto que afecte la ejecución presupuestal en un valor igual o superior al 50% * Pérdida de cobertura en la prestación de los servicios de la entidad en un valor igual o superior al 50% * Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor en un valor igual o superior al 50%. * Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor igual o superior al 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.	5
MAYOR	* Impacto que afecte la ejecución presupuestal en un valor igual o mayor al 20% e inferior al 50% * Pérdida de cobertura en la prestación de los servicios de la entidad en un valor igual o mayor al 20% e inferior al 50% * Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor igual o mayor al 20% e inferior al 50% * Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor igual o mayor al 20% e inferior al 50% 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	4
MODERADO	* Impacto que afecte la ejecución presupuestal en un valor igual o mayor al 10% y menor al 20% * Pérdida de cobertura en la prestación de los servicios de la entidad en un valor igual o mayor al 10% y menor al 20% * Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor igual o mayor al 10% y menor al 20%. * Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor igual o mayor al 10% y menor al 20% 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. - Inoportunidad en la información ocasionando retrasos en la atención a los usuarios. - Reproceso de actividades y aumento de carga operativa. - 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.	3
MENOR	* Impacto que afecte la ejecución presupuestal en un valor igual o mayor al 1% y menor al 10% * Pérdida de cobertura en la prestación de los servicios de la entidad en un valor igual o mayor al 1% y menor al 10% * Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor igual o mayor al 1% y menor al 10% * Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor igual o mayor al 1% y menor al 10% 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.	2
INSIGNIFICANTE	* Impacto que afecte la ejecución presupuestal en un valor menor al 1% * Pérdida de cobertura en la prestación de los servicios de la entidad en un valor menor al 1% * Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor menor al 1% * Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor menor al 1% 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.	1

7.3.1.2. IMPACTO RIESGOS DE CORRUPCIÓN

La medición del impacto de los riesgos de corrupción se realiza aplicando la siguiente tabla de valoración. Cada riesgo identificado es valorado de acuerdo con las preguntas la tabla y la calificación obtenida se compara con la tabla de medición de impacto de riesgo de corrupción para obtener el nivel de impacto del riesgo

No.	PREGUNTA SI EL RIESGO SE MATERIALIZA PODRÍA?	RESPUESTA	
		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 misión del sector al cual pertenece la Entidad ?		
5	¿Generar perdida de confianza de la Entidad, afectando su reputación?		
6	¿Generar perdida 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 perdida del bien o servicios o los recursos públicos?		
9	¿Generar perdida 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 perdida de credibilidad del sector?		
16	¿Ocasionar lesiones físicas o perdida de vidas humanas ?		
17	¿Afectar la imagen regional?		
18	¿Afectar la imagen nacional?		
19	¿Generar daño ambiental?		

Medición de Impacto Riesgo de Corrupción			
Descriptor	**Descripción**	**Nivel**	**Respuestas Afirmativas**
Moderado	* Afectación parcial al proceso y a la dependencia * Genera medianas consecuencias para la entidad.	5	1 – 5
Mayor	* Impacto negativo de la Entidad. * Genera altas consecuencias para la entidad.	10	6 - 11
Catastrófico	* Consecuencias desastrosas sobre el sector. * Genera consecuencias desastrosas para la entidad	20	12 - 19

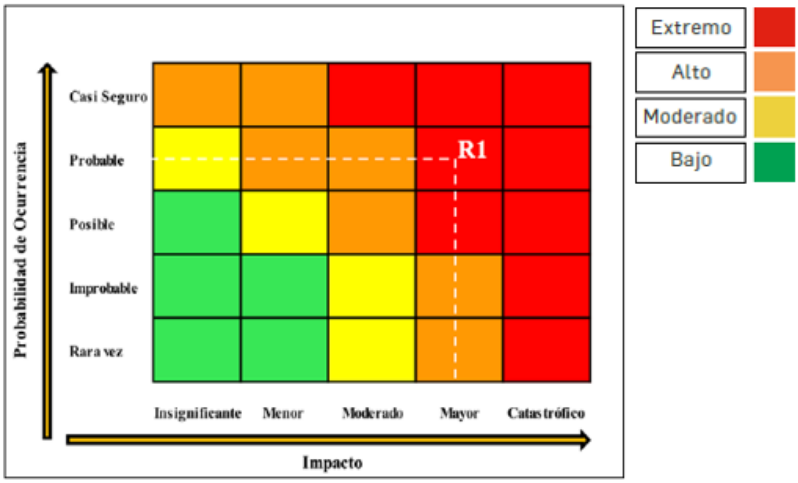
7.3.1.3. IMPACTO RIESGOS DE SEGURIDAD DIGITAL

El impacto se determina con base a la amenaza, no en las vulnerabilidades. Para tal efecto se debe tomar en consideración los aspectos contemplado en la matriz que a continuación se presenta:

Criterios de Impacto para Riesgos de Seguridad Digital			
Categoría	**Descripción Cuantitativa**	**Descripción Cualitativa**	**Nivel**
CATASTRÓFICO	*Afectación de la población en un valor igual o superior al 50% *Afectación de la ejecución presupuestal de seguridad digital en un valor igual o superior al 50% *Afectación muy grave del medio ambiente que requiere > 3 años de recuperación.	*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.	5
MAYOR	*Afectación de la población en un valor igual o mayor al 20% e inferior al 50%. *Afectación de la ejecución presupuestal de seguridad digital en un valor igual o mayor al 20% e inferior al 50% *Afectación importante del medio ambiente que requiere de 1 a 3 años de recuperación.	*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 de los empleados y terceros. *Afectación grave de la confidencialidad de la información debido al interés particular de los empleados y terceros.	4
MODERADO	*Afectación de la población en un valor igual o mayor al 10% y menor al 20%. *Afectación de la ejecución presupuestal de seguridad digital en un valor igual o mayor al 10% y menor al 20% *Afectación leve del medio ambiente requiere de 3 meses a 1 año de recuperación	*Afectación moderada de la integridad de la información debido al interés particular de los 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.	3
MENOR	*Afectación de la población en un valor igual o mayor al 1% y menor al 10%. *Afectación de la ejecución presupuestal de seguridad digital en un valor igual o mayor al 1% y menor al 10% *Afectación leve del medio ambiente requiere de 1 a 3 meses de recuperación.	*Afectación leve de la integridad. *Afectación leve de la disponibilidad. *Afectación leve de la confidencialidad.	2
INSIGNIFICANTE	*Afectación de la población en un valor menor al 1% . *Afectación de la ejecución presupuestal de seguridad digital en un valor menor al 1% *No hay afectación medioambiental.	*Sin afectación de la integridad. *Sin afectación de la disponibilidad. *Sin afectación de la confidencialidad	1

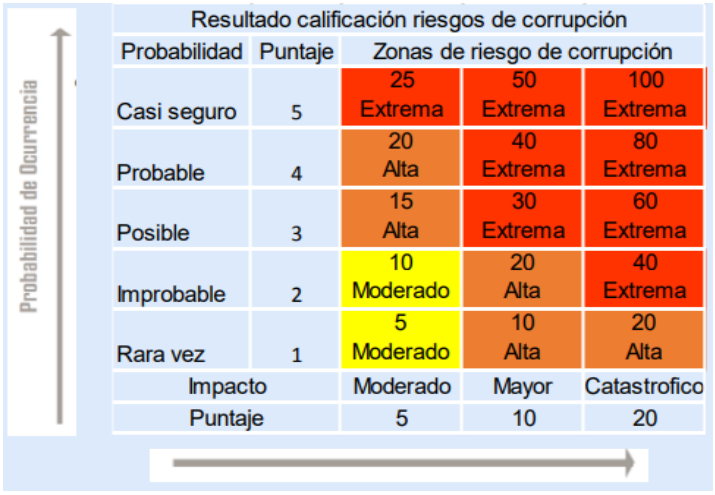
7.3.1.4. NIVEL DE ACEPTACIÓN DEL RIESGO

Acogiendo la Matriz de riesgo sugerida en la Guía de Función Pública - 2018, la calificación de la medición de los riesgos de gestión y seguridad digital se hace a través de la tabla de probabilidad e impacto así:



Fuente: *Guía de Administración de Riesgos Gestión, Corrupción y Seguridad Digital y Diseño Controles Entidades Pública V.4 2018*

Los riesgos de corrupción se hacen a través de la tabla de probabilidad e impacto así:



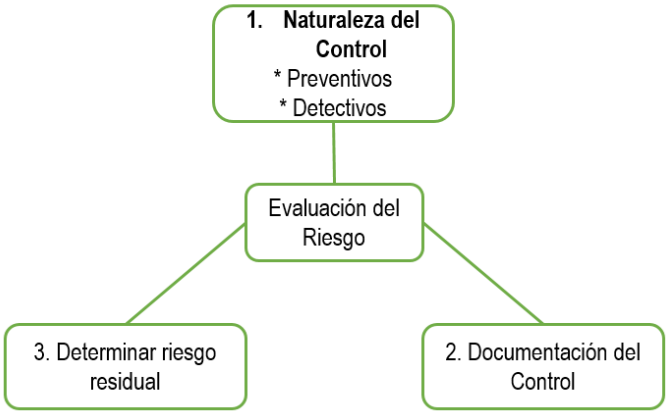
A partir de los criterios ERCA (Evitar, Reducir, Compartir y Aceptar), la Entidad establece los siguientes niveles de aceptación a los riesgos identificados:

Nivel de Aceptación		
Zona de Riesgo Residual	**Riesgos de Gestión y Seguridad Digital**	**Riesgos de Corrupción**
Bajo	**ACEPTAR** el riesgo y se administra por medio de las actividades propias del proyecto o proceso asociado.	**NINGÚN** riesgo de corrupción podrá ser aceptado.
Moderado	Se establecen acciones de Control Preventivas que permitan **REDUCIR** la probabilidad de ocurrencia del riesgo.	
Alto	Se debe incluir el riesgo tanto en el Mapa de Riesgos del Proceso como en el Mapa de Riegos Institucional y se establecen acciones de control Preventivas que permitan **EVITAR** la materialización del riesgo.	Se adoptan medidas para **REDUCIR** la probabilidad o e l impacto del riesgo, o ambos; por lo general conlleva a la implementación de controles.
Extremo	Se incluye el riesgo en el Mapa de riesgo del Proceso y en el Mapa de Riesgo Institucional, se establecen acciones de Control Preventivas y correctivas que permitan **EVITAR** la materialización del riesgo.	**Evitar** - Se abandonan las actividades que dan lugar a l riesgo, decidiendo n o iniciar o no continuar con la actividad que causa el riesgo. Se reduce la probabilidad o el impacto del riesgo, **TRANSFIRIENDO O COMPARTIENDO** una parte del riesgo.

7.3.2. EVALUACIÓN DEL RIESGO

DISEÑO DE CONTROLES

El objetivo es comparar los resultados del análisis de riesgos con los controles establecidos, para determinar la zona de riesgo final, los pasos a seguir son:



Para definir si los controles mitigan de manera adecuada el riesgo, se debe considerar diferentes aspectos a saber:

A) Persona asignada de ejecutar el control. Debe tener la autoridad, competencias y conocimientos para ejecutar el control dentro del proceso y sus responsabilidades deben ser adecuadamente segregadas o redistribuidas entre diferentes individuos para reducir así el riesgo de error o de actuaciones irregulares o fraudulentas.

B) Debe tener una periodicidad definida para su ejecución: El control debe tener una periodicidad específica para su realización, (diario, mensual, trimestral, anual) etc. y su ejecución debe ser consistente y oportuna para la mitigación del riesgo.

C) Debe indicar cuál es el propósito del control: El control debe tener un propósito que indique para qué se realiza el control, y que ese propósito conlleve a prevenir las causas que generan el riesgo (verificar, validar, conciliar, comparar, revisar, cotejar), o detectar la materialización del riesgo, y conlleve a que se realicen los ajustes y correctivos en el diseño del control o en su ejecución.

D) Debe establecer el cómo se realiza la actividad de control: El control debe indicar el cómo se realiza, de tal forma que se pueda evaluar si la fuente u origen de la información que sirve para ejecutar el control, es confiable para la mitigación del riesgo

E) Debe indicar qué pasa con las observaciones o desviaciones resultantes de ejecutar el control: El control debe indicar qué pasa con las observaciones o desviaciones como resultado de ejecutar el control

F) Debe dejar evidencia de la ejecución del control: El control debe dejar evidencia de su ejecución. Esta evidencia ayuda a que se pueda revisar la misma información por parte de un tercero y llegue a la misma conclusión de quien ejecutó el control, y se pueda evaluar que el control realmente fue ejecutado de acuerdo a los parámetros establecidos

7.3.3. ANÁLISIS Y EVALUACIÓN DEL DISEÑO DEL CONTROL

De acuerdo con las variables del diseño que debe tener cada control se pondera el peso o porcentaje que debe tener cada variable para la adecuada mitigación del riesgo, de acuerdo a la siguiente tabla:

CONTROLES DE RIESGOS						
Descripción del control	Naturaleza del Control		Criterios para la evaluación	Evaluación		
	Preventivo	Detectivo	Aspectos a evaluar en el diseño del control			
			¿Existe un responsable asignado a la ejecución del control ?	Asignado	No Asignado	
				15 %	0 %	
			¿El responsable tiene la autoridad y adecuada segregación de funciones en la ejecución del control?	Adecuado	Inadecuado	
				15 %	0 %	
			¿ La oportunidad en que se ejecuta el control ayuda a prevenir la mitigación del riesgo o a detectar la materialización del riesgo de manera oportuna?	Oportuna	Inoportuna	
				15 %	0 %	
			¿Las actividades que se desarrollan en el control realmente buscan por si sola prevenir o detectar las causas que pueden dar origen al riesgo, ejemplo Verificar, Validar Cotejar, Comparar, Revisar, etc.?	Prevenir	Detectar	No es control
				15 %	10%	0 %
			¿La fuente de información que se utiliza en el desarrollo del control es información confiable que permita mitigar el riesgo?	Confiable	No confiable	
				15%	0%	
			¿Las observaciones , desviaciones o diferencias identificadas como resultados de la ejecución del control son investigadas y resueltas de manera oportuna?	Se investigan y resuelven oportunamente	No se investigan y resuelven Oportunamente	
				15 %	0 %	
			¿Se deja evidencia o rastro de la ejecución del control, que permita a cualquier tercero con la evidencia, llegar a la misma conclusión?	Completa	Incompleta	No existe
				10 %	5 %	0 %
TOTAL				100 %		

Cada control va a tener la misma importancia, por lo tanto el consolidado de los controles para mitigar un riesgo, se realizará promediando el número de controles asociados al riesgo.

El resultado de las calificaciones del control o promedio en el diseño de los controles, que este por debajo de 96 %, se debe establecer un plan de acción, para el adecuado diseño del control. Para la calificación del diseño y ejecución de los controles, se deben tener en cuenta las siguientes tablas:

Calificación diseño de los controles	Definición
Fuerte 96% - 100%	El control o controles están bien diseñado para mitigar el Riesgo .
Moderado 86% - 95%	Con Observaciones en la evidencia del control.
Débil 0% - 85%	El control tiene debilidades en su diseño para mitigar el riesgo.

Se debe confirmar por parte de los lideres de proceso la ejecución de cada control, de acuerdo a la siguiente tabla:

Calificación ejecución de los controles	Definición
Fuerte	Siempre se ejecuta por parte de los responsables
Moderado	Algunas veces se ejecuta por parte de los responsables
Débil	Nunca se ejecuta el control

Ponderación Diseño de Controles	Ejecución Controles	*Solidez del Control*
Fuerte	Fuerte	Fuerte
	Moderado	Moderado
	Débil	Débil
Moderado	Fuerte	Moderado
	Moderado	Moderado
	Débil	Débil
Débil	Fuerte	Débil
	Moderado	Débil
	Débil	Débil

Una vez realizado el análisis y evaluación de los controles para la mitigación de los riesgos, y considerando si los controles ayudan o no a la disminución de impacto o la probabilidad, procedemos a la elaboración del Mapa de Riesgo Residual (después de los controles).

Control 1	Control 2	Control 3	Solidez del Control
Fuerte	Fuerte	Fuerte	**Fuerte**
Fuerte	Moderado	Moderado	**Moderado**
Fuerte	Débil	Débil	**Débil**
Moderado	Fuerte	Moderado	**Moderado**
Moderado	Moderado	Moderado	**Moderado**
Moderado	Débil	Débil	**Débil**
Débil	Fuerte	Débil	**Débil**
Débil	Moderado	Débil	**Débil**
Débil	Débil	Débil	**Débil**

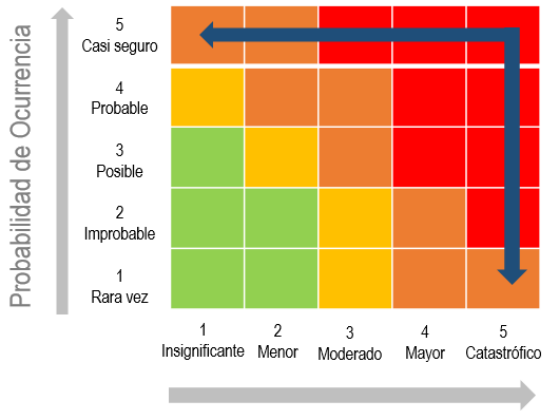
2

Calificación de los controles	Puntaje a disminuir
Débil	0
Moderado	1
Fuerte	2

1

La solidez del conjunto de controles se define acorde a la tabla por cada riesgo. Con la calificación obtenida se realiza un desplazamiento en la matriz, así: si el control afecta la **probabilidad** se avanza hacia **abajo.** Si afecta el **impacto** se avanza a la **izquierda.**

3



A partir de los criterios ERCA (Evitar, Reducir, Compartir y Aceptar), la Entidad establece la siguiente periodicidad de seguimiento a los riesgos identificados:

Zona de Riesgo Residual	Periodicidad	
	Riesgos de Gestión y Seguridad Digital	Riesgos de Corrupción
Bajo	Se realiza en el reporte **CUATRIMESTRAL** de su desempeño	Periodicidad **MENSUAL** para evitar a toda costa su materialización por parte de los procesos a cargo de los mismos.
Moderado	Se administra mediante seguimiento **CUATRIMESTRAL** y se registran sus avances la SUITE VISION EMPRESARIAL	
Alto	La Administración de estos riesgos será con periodicidad **MENSUAL** y su adecuado control se registra en la SUITE VISION EMPRESARIAL - SVE.	
Extremo	La Administración de estos riesgos será con periodicidad **MENSUAL** y su adecuado control se registra en la SUITE VISION EMPRESARIAL – SVE.	

7.3.4. ACTUALIZACIÓN Y MONITOREO AL MAPA DE RIESGOS

7.3.4.1. DISEÑO DE LOS MAPAS DE RIESGOS

Los líderes de proceso deben identificar los riesgos de su proceso de acuerdo a la metodología expresada anteriormente con el acompañamiento de la **Oficina Asesora de Planeación**. Una vez identificados y validados los riesgos de los procesos, estos se deben consignar en el formato Mapa de riesgos por Proceso**,** con su debido proceso de diligenciamiento y firmas por parte de Subdirectores y Jefes según corresponda, para la posterior publicación del Mapa de Riesgos Institucional en la página web del **HOSPITAL MILITAR CENTRAL.**

7.3.4.2. PROCESO DE ACTUALIZACIÓN Y MONITOREO

El mapa de riesgos institucional deberá ser actualizado como mínimo una vez al año o cada vez que los líderes de proceso así lo determinen, teniendo en cuenta el conocimiento sobre la evolución de la gestión o como resultado de recomendaciones provenientes de ejercicios de auditorías, o cambios en la normatividad.

Así mismo es necesario realizar el monitoreo periódico de los riesgos, teniendo en cuenta que esta actividad es de gran importancia y está a cargo de los líderes de los procesos en conjunto con sus equipos, permitiendo así asegurar la eficiencia en la administración de los riesgos del Hospital Militar Central.

Para realizar el monitoreo a los riesgos, se cuenta con el formato Seguimientos y Monitoreo Mapa de Riesgos **PL-OAPL-PR-05-FT-02**, en la cual se debe describir si el riesgo se materializó, la eficacia del control e igualmente se reportan las acciones adelantadas en caso de materializarse los riesgos.

Con el fin de consolidar los monitoreos de los riesgos se han parametrizado actividades de reporte en la plataforma Suite Visión, en la cual los líderes de proceso reportarán el comportamiento de los riesgos.

7.3.4.3. FECHAS DE REPORTE

Los líderes de proceso deben reportar los monitores de los mapas de riesgo en las siguientes fechas:

- Primer Monitoreo: Primeros diez (10) días del mes de Mayo.

- Segundo Monitoreo: Primeros diez (10) días del mes de Septiembre.
- Tercer Monitoreo: Primeros diez (10) días del mes de Enero

7.3.4.4. SEGUIMIENTO

La Oficina de Control Interno realizará seguimiento del mapa de riesgos institucional y revisará de manera independiente y objetiva el cumplimiento de los objetivos institucionales y de procesos, de acuerdo con los siguientes aspectos:

- Revisar los cambios en el "Direccionamiento estratégico" o en el entorno y cómo estos puedan generar nuevos riesgos o modificar los que ya se tienen identificados en cada uno de los procesos, con el fin de que se identifiquen y actualicen las matrices de riesgos por parte de los responsables.
- Revisión de la adecuada definición y desdoblamiento de los objetivos institucionales a los objetivos de los procesos que han servido de base para llevar a cabo la identificación de los riesgos, y realizar las recomendaciones a que haya lugar.
- Revisar que se hayan identificado los riesgos significativos que afectan en el cumplimiento de los objetivos de los procesos, además de incluir los riesgos de corrupción.
- Revisar el adecuado diseño y ejecución de los controles para la mitigación de los riesgos que se han establecido por parte de la primera línea de defensa y realizar las recomendaciones y seguimiento para el fortalecimiento de los mismos.
- Revisar el perfil de riesgo inherente y residual por cada proceso consolidado y pronunciarse sobre cualquier riesgo que este por fuera del perfil de riesgo de la entidad o que su calificación del impacto o probabilidad del riesgo no es coherente con los resultados de las auditorías realizadas.
- Para mitigar los riesgos de los procesos se encuentren documentadas y actualizadas en los procedimientos y los planes de mejora como resultado de las auditorías efectuadas, además, que se lleven a cabo de manera oportuna, se establezcan las causas raíz del problema y se evite, en lo posible, la repetición de hallazgos y la materialización de los riesgos.

8. CONTROL DE CAMBIOS

CONTROL DE CAMBIOS				
ACTIVIDADES QUE SUFRIERON CAMBIOS		OBSERVACIONES DEL CAMBIO	MOTIVOS DEL CAMBIO	FECHA DEL CAMBIO
ID	ACTIVIDAD			
1	Primera versión del Documento	N.A.	N.A.	18 de Diciembre de 2018_V1
2	Actualización Política Operativa para la Administración del Riesgo.	- Documento ajustado al formato institucional vigente. - Inclusión marco legal. - Definición de roles y responsabilidades de las líneas de defensa. - Identificación de riesgos de seguridad digital. - Análisis y evaluación del diseño del control. - Fechas de reporte.	Cambio código versión anterior: PL-OAPL-PR-05-DI-01	25 de Noviembre de 2020

APROBACIÓN				
	NOMBRE	CARGO	FECHA	FIRMA
ELABORÓ	Nicolás Corredor Ramírez	Contratista Oficina Asesora de Planeación	Diciembre de 2020	
REVISÓ	Mary Ruth Fonseca Becerra	Jefe Oficina Asesora del Sector Defensa – Oficina Asesora de Planeación	Diciembre de 2020	
	Jorge Aníbal Álvarez Chávez	Jefe Oficina de Control Interno	Diciembre de 2020	
APROBÓ	**Comité institucional de Gestión y Desempeño.**			
	Miguel Ángel Tovar Herrera	Jefe Oficina Asesora del Sector Defensa – Oficina Asesora Jurídica.	Diciembre de 2020	
	Coronel Médico. Douglas Aldemar Cáceres Castrillón	Subdirector Sector Defensa – Subdirector Médico.	Diciembre de 2020	
	Coronel Médico. (RA) Guillermo Alfredo Vega Torres	Subdirector Sector Defensa – Subdirección de Servicios Ambulatórios y de Apoyo Diagnóstico y Terapéutico	Diciembre de 2020	
	Coronel Médico. Hans Fred Garcia Araque	Subdirector Sector Defensa – Subdirección de Docencia e Investigación Científica	Diciembre de 2020	
	Coronel. César Augusto Barrios Reina	Subdirector Sector Defensa – Subdirección Administrativa del Hospital	Diciembre de 2020	
	Ingeniero. José Miguel Cortés García	Subdirector Sector Defensa – Subdirección de Finanzas	Diciembre de 2020	
	Mayor General Clara Esperanza Galvis Díaz.	Directora General de Entidad Descentralizada Adscrita al Sector Defensa	Diciembre de 2020	
PLANEACIÓN –CALIDAD Revisión Metodológica	**SMSM.** Pilar Adriana Duarte Torres	Servidor Misional de Sanidad Militar - Área Gestión de Calidad	Diciembre de 2020	