TABLA DE CONTENIDO

INTRODUCCION

El Consejo Asesor del Gobierno nacional en materia de control interno consideró necesario unificar la metodología existente para la administración del riesgo de gestión y corrupción, con el fin de hacer más sencilla la utilización de esta herramienta gerencial para las entidades públicas y así evitar duplicidades o re-procesos.

Igualmente, en respuesta a las conclusiones emitidas por la Contraloría General de la República que, producto de su labor como ente de control fiscal durante las últimas vigencias, encontró una marcada debilidad en el ejercicio del control interno efectuado por las entidades públicas, tanto del orden nacional como territorial. Es decir, se hizo evidente la importancia de fortalecer la metodología para diseñar y aplicar controles que permitan asegurar el logro de los objetivos.

Con la entrada en vigencia del modelo integrado de planeación y gestión (MIPG), que integra los sistemas de gestión de la calidad y de desarrollo administrativo; se crea un único sistema de gestión articulado con el sistema de control interno, el cual se actualiza y alinea con los mejores estándares internacionales, como son el modelo COSO 2013, COSO ERM 2017 y el modelo de las tres líneas de defensa. Lo anterior, con el fin de entregar a los ciudadanos lo mejor de la gestión y, en consecuencia, producir cambios en las condiciones de vida, mayor valor público en términos de bienestar, prosperidad general y fortalecer la lucha contra la corrupción.

1. PLANEACIÓN INSTITUCIONAL

1.1 DIRECCIONAMIENTO ESTRATEGICO

1.1.1. MISIÓN

"Prestar servicios integrales de salud de baja y mediana complejidad, en forma efectiva, oportuna, ética y con calidez humana a la población de Chaparral, su área de influencia y otras, como una organización empresarial, que nos permita una adecuada rentabilidad social y económica".

1.1.2 VISIÓN

"Ser el Hospital nivel II del Sur occidente líder del Departamento Tolima, mejorando continuamente las condiciones de calidad de vida, como una Institución sólida y acreditada que cubra sus necesidades y expectativas de salud de la comunidad".

1.1.3 OBJETIVOS ESTRATEGICOS

OBJETIVO GENERAL

El objetivo General del HOSPITAL adoptado mediante el acuerdo No. 17 noviembre de 1992.

El establecimiento público HOSPITAL SAN JUAN BAUTISTA NIVEL II tiene como objetivo general, PRESTAR SERVICIOS INTEGRALES DE SALUD, que correspondan a los procesos de promoción, prevención, tratamiento y rehabilitación, teniendo en cuenta los aspectos bio-psicosociales del individuo, la familia y la comunidad en su área de influencia.

OBJETIVOS ESTRATÉGICOS

Son objetivos específicos del HOSPITAL adoptados mediante el acuerdo N.º 17 noviembre de 1992.

1. Contribuir con soluciones concretas e integrales a los problemas de salud del Individuo, la comunidad y su entorno, mediante el diagnóstico y la implementación de los programas y actividades necesarias para tal fin.

2. Asegurar continuamente la vigencia de los principios de la participación ciudadana y comunitaria, mediante la incorporación de la familia y la comunidad a los procesos de salud.

3. Fomentar el trabajo interdisciplinario en salud, como el medio más adecuado para proporcionar una verdadera atención integral.

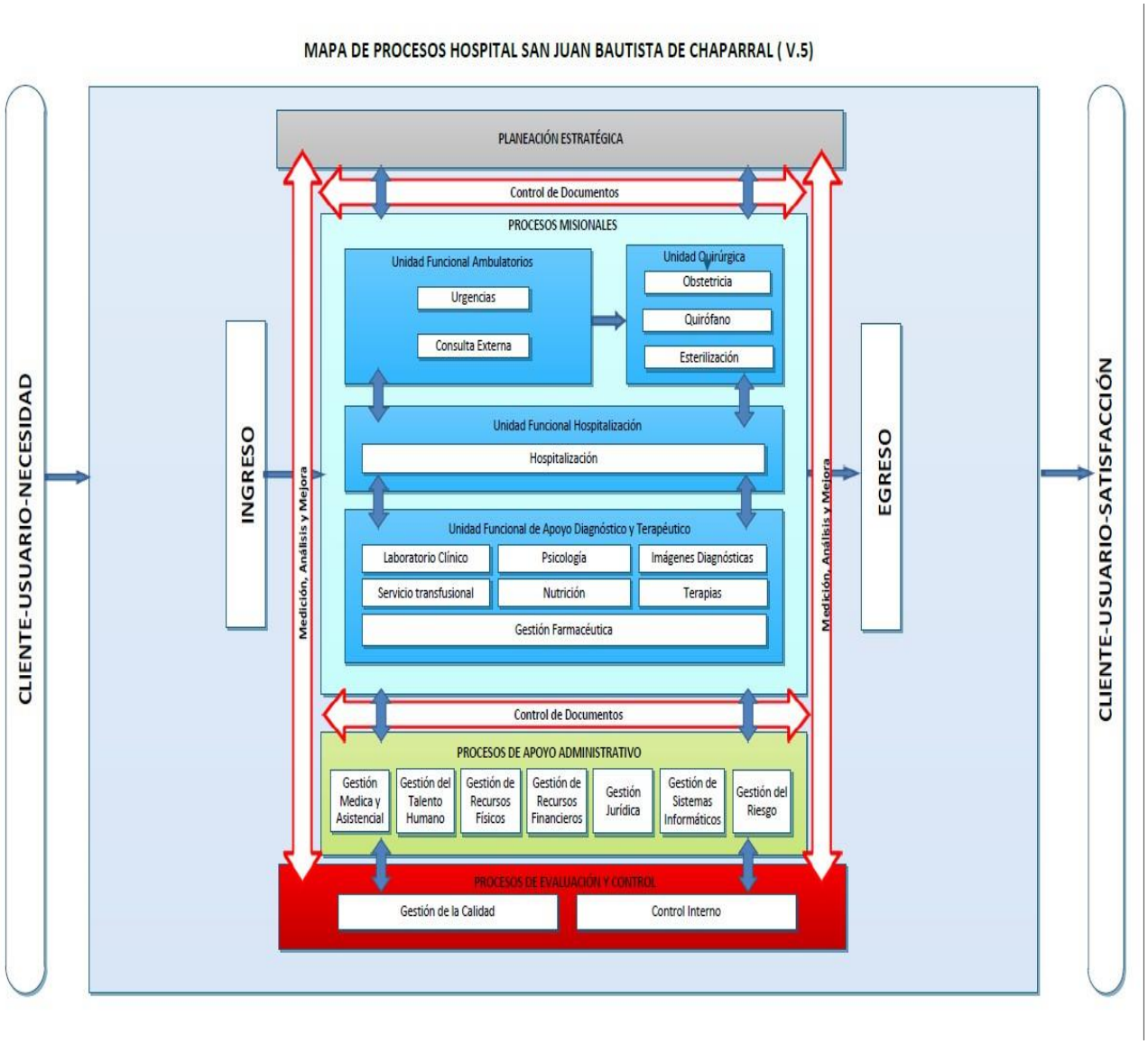
4. Promover la integración y coordinación intra y extra sectorial, en el área de influencia, evitando la duplicidad de acciones y optimizando la utilización de recursos.

5. Promover por el desarrollo integral del recurso humano, orientándolo, capacitándolo y actualizándolo continuamente, con el fin de mejorar cada vez más la calidad de atención.

6. Propender por la disminución del efecto de los desastres sobre la comunidad, mediante la elaboración y ejecución de planes de prevención y emergencias intra y extrahospitalarias.

7. Ser fuente de educación en salud para el sector y en general para toda la comunidad y líder en comprensión del fenómeno salud-enfermedad, desarrollo trabajos de investigación y evaluando periódicamente la efectividad y el impacto de los programas adelantados.

1.1.4 MAPA DE PROCESOS



1.1.4.1 CARACTERIZACIÓN DE LOS PROCESOS

Contiene la descripción del proceso y demás herramientas de enlace que son fundamentales para su desarrollo y ejecución.

MACROPROCESO: Son los procesos que soportan la estructura Institucional, y se encuentran identificados los Procesos Estratégicos, Procesos Misionales, Procesos de Apoyo y Procesos de Evaluación y Control. Según la Función Pública, cada tipo de proceso se define de la siguiente manera:

ESTRATÉGICOS
Tienen como tarea primordial el establecimiento de políticas y estrategias, fijación de objetivos, comunicación y disposición de recursos necesarios, facilitan el seguimiento y la mejora.

MISIONALES
Cadena de valor que permite obtener el resultado previsto por la entidad en el cumplimiento del objeto social o razón de ser.

APOYO
Proveen los recursos necesarios para el desarrollo de los procesos estratégicos, misionales y de evaluación.

EVALUACIÓN
Necesarios para medir y recopilar datos para el análisis del desempeño y la mejora de la eficacia y la eficiencia de la entidad.

Imagen 1. Fuente: Modelo de operación por procesos del Departamento de la Función Pública, actualizado 2017.

Imagen 2. Fuente: Modelo de operación por procesos del Departamento de la Función Pública, actualizado 2017.

1.2 POLITICA DE ADMINISTRACION DEL RIESGO

1.2.1 OBJETIVOS DE LA POLÍTICA DE ADMINISTRACIÓN DEL RIESGO

- Unificar los lineamientos en los aspectos comunes de las metodologías para la administración de todo tipo de riesgos y fortalecer el enfoque preventivo con el fin de facilitar a las entidades, la identificación y tratamiento de cada uno de ellos.

- Ofrecer herramientas para identificar, analizar, evaluar los riesgos y determinar roles y responsabilidades de cada uno de los servidores del hospital (esquema de las líneas de defensa) en los riesgos de gestión.

- Suministrar lineamientos basados en una adecuada gestión del riesgo y control a los mismos, que permitan a la alta dirección de las entidades tener una seguridad razonable en el logro de sus objetivos.

1.2.2. ALCANCE

La política de riesgos es aplicable a todos los procesos, proyectos, de la ESE y a las acciones ejecutadas por los servidores durante el ejercicio de sus funciones, con el fin de garantizar el conocimiento y control de los riesgos del Hospital.

1.2.3. TERMINOS Y DEFINICIONES

Activo: En el contexto de seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, Hardware, información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital.

Apetito al riesgo: Es el 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 de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.

Capacidad de riesgo: Es el máximo valor del nivel de riesgo que una Entidad puede soportar y a partir del cual se considera por la Alta Dirección y el Órgano de Gobierno que no sería posible el logro de los objetivos de la Entidad.

Causa: Todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.

Causa Inmediata: Circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo.

Causa Raíz: Causa principal o básica, corresponde a las razones por la cuales se puede presentar el riesgo.

Confidencialidad: Propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados.

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.

Control: Medida que permite reducir o mitigar un riesgo.

Disponibilidad: Propiedad de ser accesible y utilizable a demanda por una entidad.

Factores de Riesgo: Son las fuentes generadoras de riesgos.

Impacto: Impacto: las consecuencias que puede ocasionar a la organización la materialización del riesgo.

Integridad: Propiedad de exactitud y completitud

Mapa de riesgos: Documento con la información resultante de la gestión del riesgo.

Nivel de riesgo: Es el valor que se determina a partir de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que este evento traería sobre la capacidad institucional de alcanzar los objetivos. En general la fórmula del Nivel del Riesgo poder

ser Probabilidad * Impacto, sin embargo, pueden relacionarse las variables a través de otras maneras diferentes a la multiplicación, por ejemplo, mediante una matriz de Probabilidad – Impacto

Plan Anticorrupción y de Atención al Ciudadano: Plan que contempla la estrategia de lucha contra la corrupción que debe ser implementada por todas las entidades del orden nacional, departamental y municipal

Probabilidad: Se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. La probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.

Riesgo Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales. Nota: Los eventos potenciales hacen referencia a la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos.

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

Riesgo inherente: Nivel de riesgo propio de la actividad. El resultado de combinar la probabilidad con el impacto nos permite determinar el nivel del riesgo inherente, dentro de unas escalas de severidad

Riesgo residual: El resultado de aplicar la efectividad de los controles al riesgo inherente.

Riesgo de Seguridad de la Información: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000)

Tolerancia al riesgo: Es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del Apetito de riesgo determinado por la entidad.

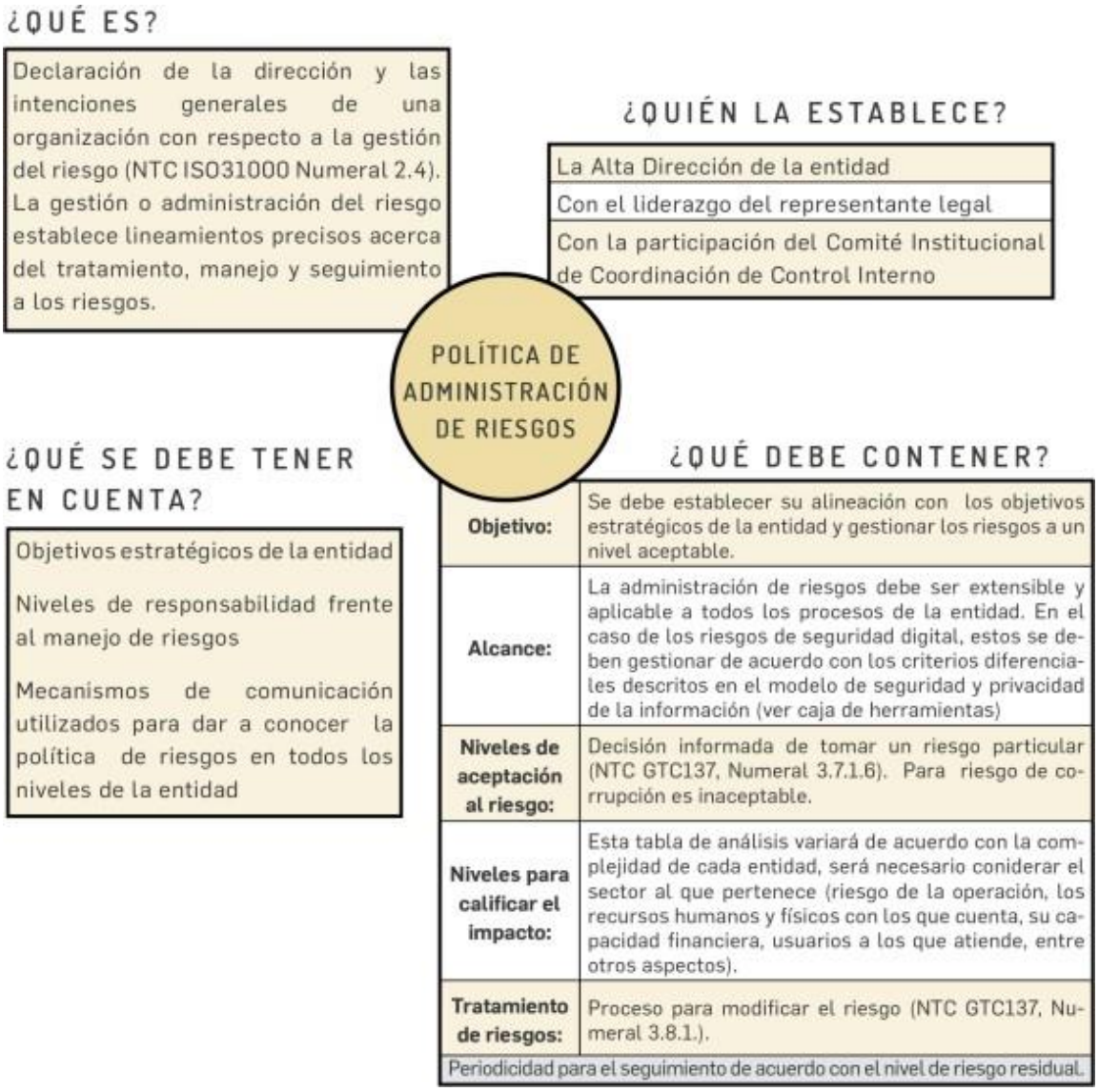
Vulnerabilidad: Representan la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.

Aceptación del riesgo: Consideración permisiva para que un riesgo continue sin controles o acciones correctivas, de mitigación y/o reducción. Sera permitido aceptar riesgos localizados en una zona de riesgo en una zona de riesgo residual baja.

1.3 IDENTIFICACIÓN DEL RIESGO

1.3.1 LINEAMIENTOS DE LA POLÍTICA DE RIESGOS

Figura 1 Estructuración de la política de administración de riesgos


¿QUÉ ES?
Declaración de la dirección y las intenciones generales de una organización con respecto a la gestión del riesgo (NTC ISO31000 Numeral 2.4). La gestión o administración del riesgo establece lineamientos precisos acerca del tratamiento, manejo y seguimiento a los riesgos.
¿QUIÉN LA ESTABLECE?
La Alta Dirección de la entidad
Con el liderazgo del representante legal
Con la participación del Comité Institucional de Coordinación de Control Interno
POLÍTICA DE ADMINISTRACIÓN DE RIESGOS
¿QUÉ SE DEBE TENER EN CUENTA?
Objetivos estratégicos de la entidad
Niveles de responsabilidad frente al manejo de riesgos
Mecanismos de comunicación utilizados para dar a conocer la política de riesgos en todos los niveles de la entidad
¿QUÉ DEBE CONTENER?
Objetivo: Se debe establecer su alineación con los objetivos estratégicos de la entidad y gestionar los riesgos a un nivel aceptable.
Alcance: La administración de riesgos debe ser extensible y aplicable a todos los procesos de la entidad. En el caso de los riesgos de seguridad digital, estos se deben gestionar de acuerdo con los criterios diferenciales descritos en el modelo de seguridad y privacidad de la información (ver caja de herramientas)
Niveles de aceptación al riesgo: Decisión informada de tomar un riesgo particular (NTC GTC137, Numeral 3.7.1.6). Para riesgo de corrupción es inaceptable.
Niveles para calificar el impacto: Esta tabla de análisis variará de acuerdo con la complejidad de cada entidad, será necesario coniderar el sector al que pertenece (riesgo de la operación, los recursos humanos y físicos con los que cuenta, su capacidad financiera, usuarios a los que atiende, entre otros aspectos).
Tratamiento de riesgos: Proceso para modificar el riesgo (NTC GTC137, Numeral 3.8.1.).
Periodicidad para el seguimiento de acuerdo con el nivel de riesgo residual.

1.3.2 IDENTIFICACION DE LOS PUNTO DE RIESGOS

Fuente: Dirección de Gestión y Desempeño Institucional de Función Pública, 2017.

1.3.3 IDENTIFICACIÓN **DE ÁREAS DEL IMPACTO**

El área de impacto es la consecuencia económica o reputacional a la cual se ve expuesta la organización en caso de materializarse un riesgo. Los impactos que aplican son afectación económica (o presupuestal) y reputacional.

1.3.3. IDENTIFICACION AREAS DE LOS FACTORES DE RIESGO

Tabla 1. Factores de riesgo

FACTOR	DEFINICIÓN	DESCRIPCIÓN
Procesos	Eventos relacionados con errores en las actividades que deben realizar los servidores de la organización.	Falta de procedimientos
		Errores en facturación
		Errores en cálculos para pagos internos y externos
		Falta de capacitación, temas relacionados con el personal

Talento humano	Incluye seguridad y salud en el trabajo. Se analiza posible dolo e intención frente a la corrupción.	Hurtos activos
		Posibles comportamientos no éticos de los empleados
		Fraude interno (corrupción, soborno)
Tecnología	Eventos relacionados con la infraestructura tecnológica de la entidad	Daño de equipos
		Caída de aplicaciones
		Caída de redes
		Errores en programas
Infraestructura	Eventos relacionados con la infraestructura física de la entidad	Derrumbes
		Incendios
		Inundaciones
		Daños a activos fijos
Evento externo	Situaciones externas que afectan la entidad.	Suplantación de identidad
		Asalto a la oficina
		Atentados, vandalismo, orden público

Fuente: Adaptado del Curso Riesgo Operativo de la Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020

1.3.4 DESCRIPCIÓN DEL RIESGO

Estructura propuesta para la redacción del riesgo

Impacto	¿Qué?	Afectación económica
Causa inmediata	¿Cómo?	Por multa y sanción del ente regulador
Causa Raíz	¿Por qué?	Debido a adquisición de bienes y servicios fuera de los requerimientos normativos

1.3.5 CLASIFICACIÓN DEL RIESGO

Ejecución y administración de procesos	Pérdidas derivadas de errores en la ejecución y administración de procesos.
Fraude externo	Pérdida derivada de actos de fraude por personas ajenas a la organización (no participa personal de la entidad).
Fraude interno	Pérdida debido a actos de fraude, actuaciones irregulares, comisión de hechos delictivos abuso de confianza, apropiación indebida, incumplimiento de regulaciones legales o internas de la entidad en las cuales está involucrado por lo menos 1 participante interno de la organización, son realizadas de forma intencional y/o con ánimo de lucro para sí mismo o para terceros.

Fallas tecnológicas	Errores en hardware, software, telecomunicaciones, interrupción de servicios básicos.
Relaciones laborales	Pérdidas que surgen de acciones contrarias a las leyes o acuerdos de empleo, salud o seguridad, del pago de demandas por daños personales o de discriminación.
Usuarios, productos y prácticas	Fallas negligentes o involuntarias de las obligaciones frente a los usuarios y que impiden satisfacer una obligación profesional frente a éstos.
Daños a activos fijos/ eventos externos	Pérdida por daños o extravíos de los activos fijos por desastres naturales u otros riesgos/eventos externos como atentados, vandalismo, orden público.

1.4 VALORACION DEL RIESGO

1.4.1 ESTRUCTURA PARA EL DESARROLLO DE LA VALORACIÓN DEL RIESGO

Fuente: Dirección de Gestión y Desempeño Institucional de Función Pública, 2018.

1.4.2 ANÁLISIS DEL RIESGO

ACTIVIDAD	FRECUENCIA DE LA ACTIVIDAD	PROBABILIDAD FRENTE AL RIESGO
Planeación estratégica	1 vez al año	Muy baja
Actividades de talento humano, jurídica, administrativa	Mensual	Media
Contabilidad, cartera	Semanal	Alta
Tecnología (incluye disponibilidad de	Diaria	Muy alta

aplicativos), tesorería		

Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020

Tabla 2. Criterios para definir el nivel de probabilidad

	Frecuencia de la Actividad	Probabilidad
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año	20%
Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año	40%
Media	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año	60%
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año	80%
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año	100%

Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

Tabla 3. Impacto

	Afectación Económica	Reputacional
Leve 20%	Afectación menor a 10 SMLMV .	El riesgo afecta la imagen de algún área de la organización.
Menor-40%	Entre 10 y 50 SMLMV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de junta directiva y accionistas y/o de proveedores.
Moderado 60%	Entre 50 y 100 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.
Mayor 80%	Entre 100 y 500 SMLMV	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal.
Catastrófico 100%	Mayor a 500 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país

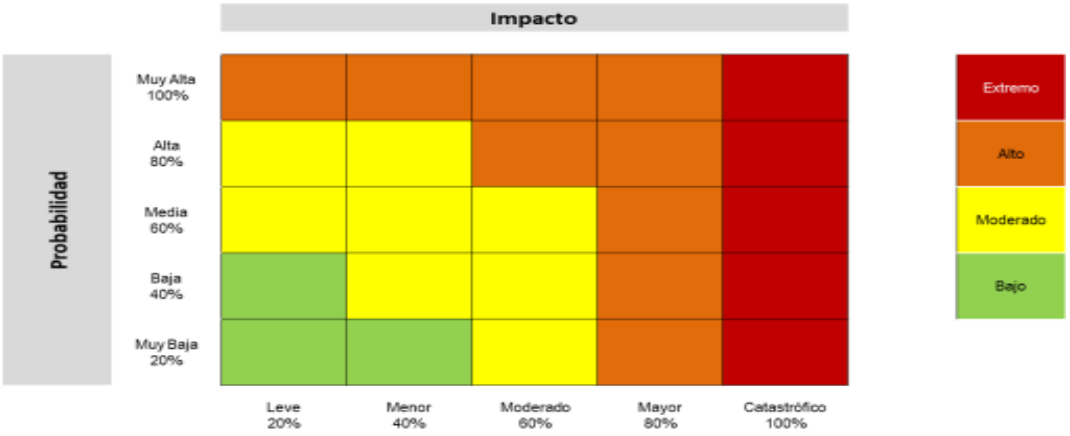
Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

1.5 EVALUACIÓN DE RIESGOS

A partir del análisis de la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto s, se busca determinar la zona de riesgo inicial (RIESGO INHERENTE).

1.5.1 ANÁLISIS PRELIMINAR (RIESGO INHERENTE): se trata de determinar los niveles de severidad a través de la combinación entre la probabilidad y el impacto.

Figura 1 Mapa de calor



Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

1.5.2 VALORACIÓN DE CONTROLES: La medida que permite reducir o mitigar el riesgo. Para la valoración de controles se debe tener en cuenta:

La identificación de controles se debe realizar a cada riesgo a través de las entrevistas con los líderes de procesos o servidores expertos en su quehacer. En este caso sí aplica el criterio experto.

Los responsables de implementar y monitorear los controles son los líderes de proceso con el apoyo de su equipo de trabajo.

1.5.3 ESTRUCTURA PARA LA DESCRIPCIÓN DEL CONTROL

- Responsable de ejecutar el control: Identifica el cargo del servidor que ejecuta el control, en caso de que sean controles automáticos se identificará el sistema que realiza la actividad.
- Acción: se determina mediante verbos que indican la acción que deben realizar como parte del control.
- Complemento: corresponde a los detalles que permiten identificar claramente el objeto del control.

1.5.4 TIPOLOGÍA DE CONTROLES Y LOS PROCESOS

- Control preventivo: Control accionado en la entrada del proceso y antes de que se realice la actividad originadora del riesgo, se busca establecer las condiciones que aseguren el resultado final esperado.

- Control detectivos: Control accionado durante la ejecución del proceso. Estos controles detectan el riesgo, pero generan reprocesos.
- Control correctivo: Control accionado en la salida del proceso y después de que se materializa el riesgo. Estos controles tienen costos implícitos.

De acuerdo con la forma como se ejecutan tenemos:

- Control manual: controles que son ejecutados por personas.
- Control automático: son ejecutados por un sistema.

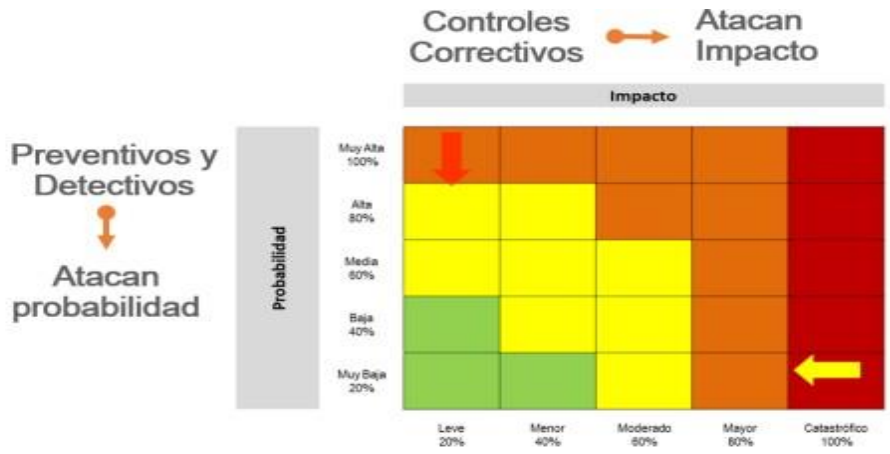
1.5.5 ATRIBUTOS PARA EL DISEÑO DE CONTROLES

Tabla 4

Características			Descripción	Peso
Atributos de eficiencia	Tipo	Preventivo	Va hacia las causas del riesgo, aseguran el resultado final esperado.	25%
		Detectivo	Detecta que algo ocurre y devuelve el proceso a los controles preventivos. Se pueden generar reprocesos.	15%
		Correctivo	Dado que permiten reducir el impacto de la materialización del riesgo, tienen un costo en su implementación.	10%
	Implementación	Automático	Son actividades de procesamiento o validación de información que se ejecutan por un sistema y/o aplicativo de manera automática sin la intervención de personas para su realización.	25%
		Manual	Controles que son ejecutados por una persona, tiene implícito el error humano.	15%
*Atributos informativos	Documentación	Documentado	Controles que están documentados en el proceso, ya sea en manuales, procedimientos, flujogramas o cualquier otro documento propio del proceso.	-
		Sin documentar	Identifica a los controles que pese a que se ejecutan en el proceso no se encuentran documentados en ningún documento propio del proceso.	-
	Frecuencia	Continua	El control se aplica siempre que se realiza la actividad que conlleva el riesgo.	-
		Aleatoria	El control se aplica aleatoriamente a la actividad que conlleva el riesgo	-
	Evidencia	Con registro	El control deja un registro permite evidencia la ejecución del control.	-
		Sin registro	El control no deja registro de la ejecución del control.	-

Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

1.5.6 MOVIMIENTO EN LA MATRIZ DE CALOR ACORDE CON EL TIPO DE CONTROL



Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

1.5.7 ESTRATEGIAS PARA COMBATIR EL RIESGO

Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

1.6 HERRAMIENTAS PARA LA GESTIÓN DEL RIESGO

1.6.1 GESTIÓN DE EVENTOS

Se pueden considerar incidentes que generan o podrían generar pérdidas a la entidad se debe contar con una base histórica de eventos ermita revisar si el riesgo fue identificado y qué sucedió con los controles. En caso de que el riesgo no se hubiese identificado, se debe incluir y dar el tratamiento correspondiente de acuerdo con la metodología.

1.7 MONITOREO Y REVISIÓN

Fuente: Dirección de Gestión y Desempeño Institucional de Función Pública, 2018.

1.7.1 LINEAMIENTOS SOBRE LOS RIESGOS RELACIONADOS CON POSIBLES ACTOS DE CORRUPCIÓN

De acuerdo con la siguiente 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 de definición de riesgo de corrupción

1.7.2 RIESGOS DE CORRUPCIÓN

Elaborado por: Prof	MATRIZ: DEFINICIÓN DEL RIESGO DE CORRUPCIÓN				Gestión y
Revisado por: Com - MIPG	**Descripción del riesgo**	**Acción u omisión**	**Uso del poder**	**Desviar la gestión de lo público**	**Beneficio privado**
	Posibilidad de recibir o solicitar cualquier dádiva				

- Se elabora anualmente por cada responsable de los procesos.
- Consolidación: La oficina de planeación, quien haga sus veces, lidera el proceso de administración de estos y es la encargada de consolidar el mapa de riesgos de corrupción.
- Publicación del mapa de riesgos de corrupción: se debe publicar en la página web de la entidad, en la sección de transparencia y acceso a la información.
- Socialización: Los servidores públicos y contratistas de la entidad deben conocer el mapa de riesgos de corrupción antes de su publicación. Para lograr este propósito la oficina de planeación o quien haga sus veces, deberá diseñar y poner en marcha las actividades o mecanismos necesarios para que los funcionarios y contratistas conozcan, debatan y formulen sus apreciaciones y propuestas sobre el proyecto del mapa de riesgos de corrupción.
- Ajustes y modificaciones: se podrán llevar a cabo los ajustes y modificaciones necesarias orientadas a mejorar el mapa de riesgos de corrupción después de su publicación y durante el respectivo año de vigencia.
- Monitoreo: en concordancia con la cultura del autocontrol al interior de la entidad, los líderes de los procesos junto con su equipo realizarán monitoreo y evaluación permanente a la gestión de riesgos de corrupción
- Seguimiento: El Asesor (a) de control interno o quien haga sus veces debe adelantar seguimiento a la gestión de riesgos de corrupción.

1.7.3 ANÁLISIS DE LA PROBABILIDAD

La 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.

La 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

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

(Fuente DAFP)

1.7.4 ANÁLISIS DEL IMPACTO

El impacto se debe analizar y calificar a partir de las consecuencias identificadas en la fase de descripción del riesgo

Criterios para calificar el impacto en riesgos de corrupción

N.°	PREGUNTA: SI EL RIESGO DE CORRUPCIÓN SE MATERIALIZA PODRÍA...	RESPUESTA SÍ	RESPUESTA NO
1	¿Afectar al grupo de funcionarios del proceso?	X	
2	¿Afectar el cumplimiento de metas y objetivos de la dependencia?	X	
3	¿Afectar el cumplimiento de misión de la entidad?	X	
4	¿Afectar el cumplimiento de la misión del sector al que pertenece la entidad?		X
5	¿Generar pérdida de confianza de la entidad, afectando su reputación?	X	
6	¿Generar pérdida de recursos económicos?	X	
7	¿Afectar la generación de los productos o la prestación de servicios?	X	
8	¿Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien, servicios o recursos públicos?		X
9	¿Generar pérdida de información de la entidad?		X
10	¿Generar intervención de los órganos de control, de la Fiscalía u otro ente?	X	
11	¿Dar lugar a procesos sancionatorios?	X	
12	¿Dar lugar a procesos disciplinarios?	X	
13	¿Dar lugar a procesos fiscales?	X	
14	¿Dar lugar a procesos penales?		X
15	¿Generar pérdida de credibilidad del sector?		X
16	¿Ocasionar lesiones físicas o pérdida de vidas humanas?		X
17	¿Afectar la imagen regional?		X
18	¿Afectar la imagen nacional?		X
19	¿Generar daño ambiental?		X
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.		10	
MODERADO	Genera medianas consecuencias sobre la entidad		
MAYOR	Genera altas consecuencias sobre la entidad.		
CATASTRÓFICO :	Genera consecuencias desastrosas para la entidad		

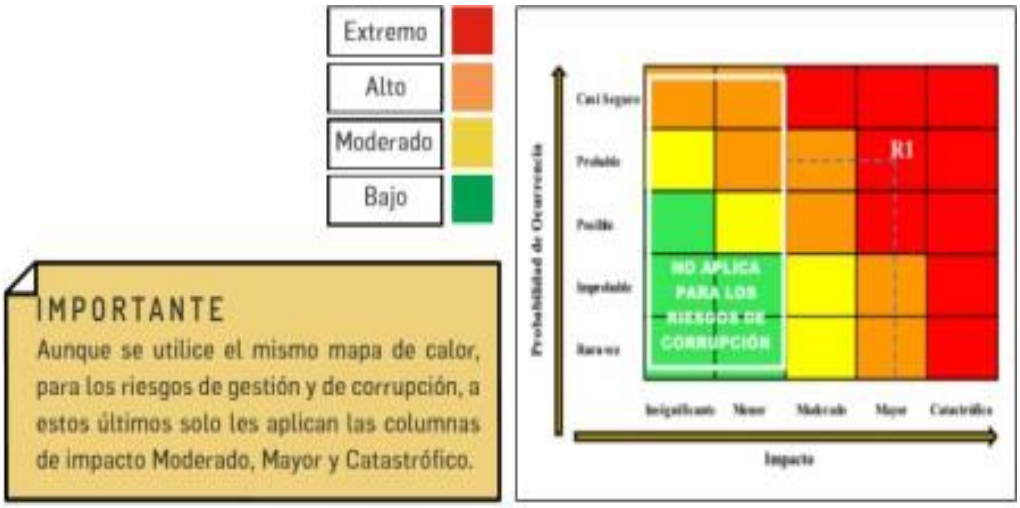
Nivel de impacto MAYOR

Fuente: Secretaría de Transparencia de la Presidencia de la República.

1.7.5 ANÁLISIS DEL IMPACTO EN RIESGOS DE CORRUPCIÓN

Para los riesgos de corrupción, el análisis de impacto se realizará teniendo en cuenta solamente los niveles “moderado”, “mayor” y “catastrófico”

Por último, ubique en el mapa de calor el punto de intersección resultante de la probabilidad y el impacto para establecer el nivel del riesgo inherente.



Fuente: Secretaría de Transparencia de la Presidencia de la República.

1.8 TRATAMIENTO DEL RIESGO

Fuente: DAFP

ACEPTAR EL RIESGO: Es importante aclarar que en caso de riesgos de corrupción estos no pueden ser aceptados.

EVITAR EL RIESGO: No se considera como una opción

COMPARTIR EL RIESGO: No es posible transferir la responsabilidad del riesgo.

REDUCIR EL RIESGO: El nivel de riesgo debería ser administrado mediante el establecimiento de controles, de modo que el riesgo residual se pueda reevaluar como algo aceptable para la entidad. Estos controles disminuyen normalmente la probabilidad y/o el impacto del riesgo.

TRATAMIENTO DEL RIESGO: Rol que le corresponde a la primera línea de defensa el establecimiento de actividades de control.

(Fuente DAFP)

MONITOREO DE RIESGOS DE CORRUPCIÓN: Los líderes de los procesos deben monitorear y revisar periódicamente la gestión de riesgos de corrupción, la oficina de planeación adelantar el monitoreo (segunda línea de defensa), para este propósito se sugiere elaborar una matriz. Dicho monitoreo será en los tiempos que determine la entidad.

REPORTE DE LA GESTIÓN DEL RIESGO DE CORRUPCIÓN: Se debe reportar en el mapa y plan de tratamiento de riesgos los riesgos de corrupción, de tal manera que se comunique toda la información necesaria para su comprensión y tratamiento adecuado.

SEGUIMIENTO DE RIESGOS DE CORRUPCIÓN: Seguimiento: El Asesor (a) de Control Interno o quien haga sus veces, debe adelantar seguimiento al Mapa de Riesgos de Corrupción.

En este sentido es necesario que adelante seguimiento a la gestión del riesgo, verificando la efectividad de los controles.

- Primer seguimiento: Con corte al 30 de abril. En esa medida, la publicación deberá surtirse dentro de los diez (10) primeros días del mes de mayo.
- Segundo seguimiento: Con corte al 31 de agosto. La publicación deberá surtirse dentro de los diez (10) primeros días del mes de septiembre.

- Tercer seguimiento: Con corte al 31 de diciembre. La publicación deberá surtirse dentro de los diez (10) primeros días del mes de enero.

El seguimiento adelantado por la Oficina de Control Interno se deberá publicar en la página web de la entidad o en un lugar de fácil acceso para el ciudadano.

En especial deberá adelantar las siguientes actividades:

- Verificar la publicación del Mapa de Riesgos de Corrupción en la página web de la entidad.

- Seguimiento a la gestión del riesgo.
- Revisión de los riesgos y su evolución.
- Hay que asegurar que los controles sean efectivos, le apunten al riesgo y estén funcionando en forma adecuada

Acciones para seguir en caso de materialización de riesgos de corrupción

En el evento de materializarse un riesgo de corrupción, es necesario realizar los ajustes necesarios con acciones, tales como:

1) Informar a las autoridades de la ocurrencia del hecho de corrupción.

2) Revisar el mapa de riesgos de corrupción, en particular, las causas, riesgos y controles.

3) Verificar si se tomaron las acciones y se actualizó el mapa de riesgos de corrupción.

4) Llevar a cabo un monitoreo permanente. La Oficina de Control Interno debe asegurar que los controles sean efectivos, le apunten al riesgo y estén funcionando en forma oportuna y efectiva.

Las acciones adelantadas se refieren a:

- Determinar la efectividad de los controles.
- Mejorar la valoración de los riesgos.
- Mejorar los controles.
- Analizar el diseño e idoneidad de los controles y si son adecuados para prevenir o mitigar los riesgos de corrupción.
- Determinar si se adelantaron acciones de monitoreo.
- Revisar las acciones del monitoreo.

1.9 LINEAMIENTOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Se debe tener en cuenta que la política de seguridad digital se vincula al modelo de seguridad y privacidad de la información (MSPI), el cual se encuentra alineado con el marco de referencia de arquitectura TI y soporta transversalmente los otros habilitadores de la política de gobierno digital: seguridad de la información, arquitectura, servicios ciudadanos digitales

1.9.1 IDENTIFICACIÓN DE LOS ACTIVOS DE SEGURIDAD DE LA INFORMACIÓN

Es necesario identificar los activos de información del proceso.

Figura 2. Conceptualización activos de información

¿Qué son los activos?	¿Por qué identificar los activos?
Un activo es cualquier elemento que tenga valor para la organización, sin embargo, en el contexto de seguridad digital, son activos elementos tales como: -Aplicaciones de la organización	Permite determinar **qué es lo más importante que cada entidad y sus procesos poseen** (sean bases de datos, archivos, servidores web o aplicaciones clave para que la entidad pueda prestar sus servicios).

Fuente: Actualizado por la Dirección de Gestión y Desempeño Institucional de Función Pública y Ministerio TIC, 2020

Figura 3. Pasos para la identificación de activos

Fuente: Actualizado por la Dirección de Gestión y Desempeño Institucional de Función Pública y Ministerio TIC, 2020

1.9.2 IDENTIFICACIÓN DEL RIESGO

Se podrán identificar los siguientes tres (3) riesgos inherentes de seguridad de la información:

- Pérdida de la confidencialidad
- Pérdida de la integridad
- Pérdida de la disponibilidad

Tabla 4 de amenazas y vulnerabilidades de acuerdo con el tipo de activo

Tipo de activo	Ejemplos de vulnerabilidades	Ejemplos de amenazas
Hardware	Almacenamiento de medios sin protección	Hurto de medios o documentos
Software	Ausencia de parches de seguridad	Abuso de los derechos
Red	Líneas de comunicación sin protección	Escucha encubierta
Información	Falta de controles de acceso físico	Hurto de información

Tipo de activo	Ejemplos de vulnerabilidades	Ejemplos de amenazas
Personal	Falta de capacitación en las herramientas	Error en el uso
Organización	Ausencia de políticas de seguridad	Abuso de los derechos

Fuente: Ministerio de Tecnologías de la Información y Comunicaciones Min TIC, 2018.

Figura 4 Formato de descripción del riesgo de seguridad de la información

Seleccionar las vulnerabilidades asociadas a la amenaza identificada

RIESGO	ACTIVO	DESCRIPCIÓN DEL RIESGO	AMENAZA	TIPO	CAUSAS/ VULNERA-BILIDADES	CONSECUENCIAS
Base de datos de nómina	Pérdida de la integridad	La falta de políticas de seguridad digital, ausencia de políti-cas de control de acceso, contraseñas sin protección y mecanismos de autenticación débil, pueden facilitar una modificación no autorizada, lo cual causaría la pérdida de la integridad de la base de datos de nómina.	Modificación no autorizada	Seguridad digital	Falta de políticas de seguridad digital	Posibles consecuencias que pueda enfrentar la entidad o el proceso a causa de la materialización del riesgo(legales, económicas, sociales, reputacionales, confianza en el ciudadano). Ej.: posible retraso en el pago de nómina.
					Ausencia de políticas de control de acceso	
					Contraseñas sin protección	
					Autenticación débil	

IMPORTANTE

- Existirían tres (3) tipos de riesgos: pérdida de confidencialidad, pérdida de la integridad y pérdida de la disponibilidad de los activos. Para cada tipo de riesgo se podrán seleccionar las amenazas y las vulnerabilidades que puedan causar que dicho riesgo se materialice.
- Los catálogos de amenazas y vulnerabilidades comunes se encuentran en la sección 4.1.7. del **anexo "Lineamientos para la gestión del riesgo de seguridad digital en entidades públicas"**, el cual hace parte de la presente guía.
- **NOTA 1:** tener en cuenta que la agrupación de activos debe ser del mismo tipo, por ejemplo, analizar conjuntamente activos tipo hardware, software, información, entre otros, para determinar amenazas y vulnerabilidades comunes que puedan afectar a dicho grupo.
- **NOTA 2:** las entidades públicas deben incluir como mínimo los procesos y procedimientos establecidos en esta guía. Aquellas entidades que ya estén adelantando procesos relacionados con la gestión de este tipo de riesgo y que incorporen al menos lo dispuesto en estas guías podrán continuar bajo sus procedimientos. Si alguno de los aspectos contenidos en esta guía no está contemplado, deberá ser agregado a los que manejan actualmente.

Fuente: Elaboración conjunta entre la Dirección de Gestión y Desempeño Institucional de Función Pública y el Ministerio TIC, 2018.

1.9.3 VALORACIÓN DEL RIESGO

	Frecuencia de la Actividad	Probabilidad
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año	20%
Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año	40%
Media	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año	60%
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año	80%
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año	100%

El impacto se entiende como la consecuencia económica y reputacional que se genera por la materialización del riesgo.

	Afectación Económica	Reputacional
Leve 20%	Afectación menor a 10 SMLMV .	El riesgo afecta la imagen de algún área de la organización.
Menor-40%	Entre 10 y 50 SMLMV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de junta directiva y accionistas y/o de proveedores.
Moderado 60%	Entre 50 y 100 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.
Mayor 80%	Entre 100 y 500 SMLMV	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal.
Catastrófico 100%	Mayor a 500 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país

El análisis preliminar (riesgo inherente), en esta etapa se define el nivel de severidad para el riesgo de seguridad de la información identificado

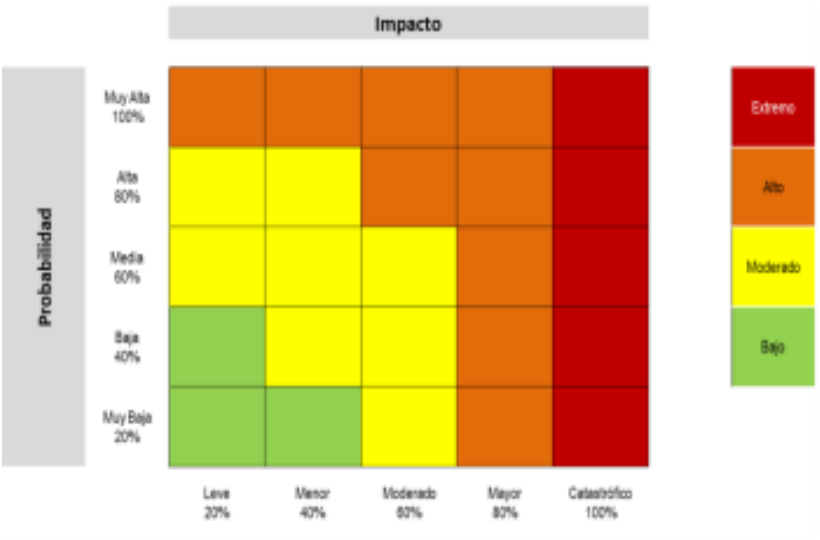


Figura 5

IMPORTANTE

Cada entidad deberá adaptar los criterios a su realidad.
El nivel de impacto deberá ser determinado con la presencia de cualquiera de los criterios establecidos, tomando el criterio con mayor nivel de afectación, ya sea cualitativo o cuantitativo.

Las variables confidencialidad, integridad y disponibilidad se definen de acuerdo con el modelo de seguridad y privacidad de la información de la estrategia de Gobierno Digital (GD) del Ministerio de Tecnologías de la Información y las Comunicaciones.

La variable población se define teniendo en cuenta el establecimiento del contexto externo de la entidad, es decir, que la consideración de población va a estar asociada a las personas a las cuales se les prestan servicios o trámites en el entorno digital y que de una u otra forma pueden verse afectadas por la materialización de algún riesgo en los activos identificados. Los porcentajes en las escalas pueden variar, según la entidad y su contexto.

La variable presupuesto es la consideración de presupuesto afectado por la entidad debido a la materialización del riesgo, contempla sanciones económicas o impactos directos en la ejecución presupuestal.

La variable ambiental estará también alineada con la afectación del medio ambiente por la materialización de un riesgo de seguridad digital. Esta variable puede no ser utilizada en la mayoría de los casos, pero debe tenerse en cuenta, ya que en alguna eventualidad puede existir afectación ambiental.

RIESGO	ACTIVO	AMENAZA	VULNERABILIDAD	PROBABILIDAD	IMPACTO	ZONA DE RIESGO
Pérdida de la Confidencialidad	Base de datos de nómina	Modificación no autorizada	Ausencia de políticas de control de acceso	4-Probable	4- Mayor	Extrema
			Contraseñas sin protección			
			Ausencia de mecanismos de identificación y autenticación de usuarios			
			Ausencia de bloqueo de sesión			

Fuente: Adaptado de Instituto de Auditores Internos. COSO ERM. Agosto 2004.

IMPORTANTE:
La probabilidad y el impacto se determinan con base a la amenaza, no en las vulnerabilidades.

Fuente: Elaboración conjunta entre la Dirección de Gestión y Desempeño Institucional de Función Pública y el Ministerio TIC, 2018.

1.9.4 Controles asociados a la seguridad de la información

Procedimientos operacionales y responsabilidades	Objetivo: asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información
Procedimientos de operación documentados	Control: los procedimientos de operación se deberían documentar y poner a disposición de todos los usuarios que los necesiten.
Gestión de cambios	Control: se deberían controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.
Gestión de capacidad	Control: para asegurar el desempeño requerido del sistema se debería hacer seguimiento al uso de los recursos, llevar a cabo los ajustes y las proyecciones de los requisitos sobre la capacidad futura.
Separación de los ambientes de desarrollo, pruebas y operación	Control: se deberían separar los ambientes de desarrollo, prueba y operación para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.
Protección contra códigos maliciosos	Objetivo: asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.
Controles contra códigos maliciosos	Control: se deberían implementar controles de detección, prevención y recuperación, combinados con la toma de conciencia apropiada por parte de los usuarios para protegerse contra códigos maliciosos.
Copias de respaldo	Objetivo: proteger la información contra la perdida de datos.
Respaldo de información	Control: se deberían hacer copias de respaldo de la información, del *software* y de las imágenes de los sistemas, ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada.

Fuente: Ministerio de Tecnologías de la Información y Comunicaciones Min TIC 2018.

Figura 6

N.	RIESGO	ACTIVO	TIPO	AMENAZAS	TIPO	PROBABILIDAD	IMPACTO	RIESGO RESIDUAL	OPCIÓN TRATAMIENTO	ACTIVIDAD DE CONTROL	SOPORTE	RESPONSABLE	TIEMPO	INDICADOR
2	**Pérdida de la integridad**	Base de datos de nómina	Seguridad digital	Modificación no autorizada	Ausencia de políticas de control de acceso	**Probable**	**Menor**	**Moderado**	Reducir	A.9.1.1 Política de control de acceso	Política creada y comunicada	Oficina TI	Tercer trimestre de 2018	**EFICACIA:** Índice de cumplimiento actividades= (# de actividades cumplidas / # de actividades programadas) x 100 **EFECTIVIDAD:** Efectividad del plan de manejo de riesgos= (# de modificaciones no autorizadas)
					Contraseñas sin protección				Reducir	A.9.4.3 Sistema de gestión de contraseñas	Procedimientos para la gestión y protección de contraseñas	Oficina TI	Tercer trimestre de 2018	
					Ausencia de mecanismos de identificación y autenticación de usuarios				Reducir	A 9.4.2 Procedimiento de ingreso seguro	Procedimiento para ingreso seguro	Oficina TI	Tercer trimestre de 2018	
					"Ausencia de bloqueo				Reducir	A.11.2.8 Equipos de usuario desatendidos	Configuraciones para bloqueo automático de sesión	Oficina TI	Tercer trimestre de 2018	

*En este ejemplo el responsable de las actividades de control fue la Oficina de TI, sin embargo existen actividades para el área de personal, recursos físicos o cada oficina en particular. El análisis de riesgos determinará los controles y los responsables en cada caso.

Fuente: Elaboración conjunta entre la Dirección de Gestión y Desempeño Institucional de Función Pública y el Ministerio TIC, 2018.

BIBLIOGRAFÍA

Celis, Ó. B. (2012). Gestión Integral de Riesgos. Bogotá D.C.: Consorcio Gráfico Ltda.

COSO Committee of Sponsoring Organizations of the Treadway Commission. (2017). Enterprise Risk Management. Integrating with Strategy and Performance. Durham: Association of International Certified Professional Accountants.

ICONTEC Internacional. (2011). NORMA TÉCNICA COLOMBIANA GTC 137. GESTIÓN DEL RIESGO. VOCABULARIO. Bogotá D.C.: Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC).

ICONTEC Internacional. (2011). NORMA TÉCNICA COLOMBIANA NTC ISO 31000. GESTIÓN DEL RIESGO. PRINCIPIOS Y DIRECTRICES. Bogotá D.C.: Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC).

ICONTEC Internacional. (2013). NORMA TÉCNICA COLOMBIANA NTC-IEC/ISO 31010. GESTION DE RIESGOS. TÉCNICAS DE VALORACIÓN DEL RIESGO. Bogotá D.C.: Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC).

Instituto de Auditores Internos de Colombia. (2017). MARCO INTERNACIONAL PARA LA PRÁCTICA PROFESIONAL DE LA AUDITORÍA INTERNA. Bogotá D.C.
https://www.mintic.gov.co/gestión-ti/Seguridad-TI/Modelo-de-Seguridad/

1. ANEXO MAPA DE RIESGOS INSTITUCIONAL

CODIGO: OADS-F-13 VERSIÓN: 2	MAPA DE RIESGOS INSTITUCIONAL 2023																				
						RIESGO INHERENTE			Controles existentes			Riesgo residual									
MACROPROCESO	PROCESO	CLASIFICACION DEL RIESGO	NOMBRE DEL RIESGO	CAUSAS (INTERNAS O EXTERNA)	CONSECUENCIAS (Legales, económicas, Jurídicas etc.)	Probabilidad	Impacto	Nivel	Herramientas	Manuales, guías, procedimientos	Responsable	Probabilidad	Impacto	Nivel	Opción de manejo	Acciones preventivas	Peso de la Acción (%)	Periodo de seguimiento	Fecha de inicio	Fecha de Terminación	Acción de contingencia ante posible materialización

CONTROL DE CAMBIOS

VERSIÓN	*FECHA*	*DESCRIPCIÓN DE LA ACTUALIZACIÓN*
2	28/11/2018	ACTUALIZACIÓN CON LA NORMA
3	17/08/2022	ACTUALIZACIÓN CON LA NORMA
4	23/02/2023	CAMBIOS EN MAPA DE RIESGOS