Tribunal Supremo de Elecciones
PILAR DE LA DEMOCRACIA

GUÍA
METODOLÓGICA PARA LA GESTIÓN DE RIESGOS DEL SIVAR

Dirección EJECUTIVA
TRIBUNAL SUPREMO DE ELECCIONES

Unidad de Control Interno

Tabla de contenidos

1. Introducción

El Sistema de Identificación, Valoración y Administración de Riesgos, (en adelante SIVAR) fue aprobado por el Tribunal Supremo de Elecciones, (en adelante TSE); en sesión ordinaria n.° 124-2005 del 22 de diciembre de 2005, comunicado en el oficio n.° 8295-TSE-2005, del 23 de diciembre de 2005; y fue implementado a partir de enero de 2007, según se desprende del oficio n.° 0227-TSE-2007 del 16 de enero de 2007, para dar cumplimiento a lo establecido en el artículo 18 de la Ley General de Control Interno, sobre el Sistema Específico de Valoración de Riesgos Institucional, (SEVRI).

De conformidad con lo anterior y con las Normas de control interno para el Sector Público:

> N-2-2009-CO-DFOE, emitidas por la Contraloría General de la República, se ha actualizado esta guía metodológica para la gestión de riesgos del SIVAR, con el propósito de que las personas responsables de completar las matrices de valoración de riesgos de las unidades administrativas, cuenten con la información requerida para esa gestión; en ella se detallan cada una de las actividades para cumplir satisfactoriamente dicho instrumento.

Importa recordar que es responsabilidad del jerarca y de las personas titulares subordinadas, según sus competencias, *"diseñar, adoptar, evaluar y perfeccionar como parte del SCI; las actividades de control pertinentes"* (Pág. 13 NCISP) con el fin de evitar o mitigar los riesgos; así como velar por el cumplimiento de las acciones correctivas y el seguimiento del Sistema de Identificación, Administración y Valoración de Riesgos (SIVAR).

2. Alcance

El Sistema Específico de Valoración de Riesgo Institucional (SEVRI), es de acatamiento obligatorio para las instituciones públicas, quienes deben establecer y mantener su funcionamiento. En el TSE se implementa el Sistema de Identificación, Valoración y Administración del Riesgo (SIVAR) que abarca a todas las unidades administrativas que lo conforman.

3. Normativa aplicable

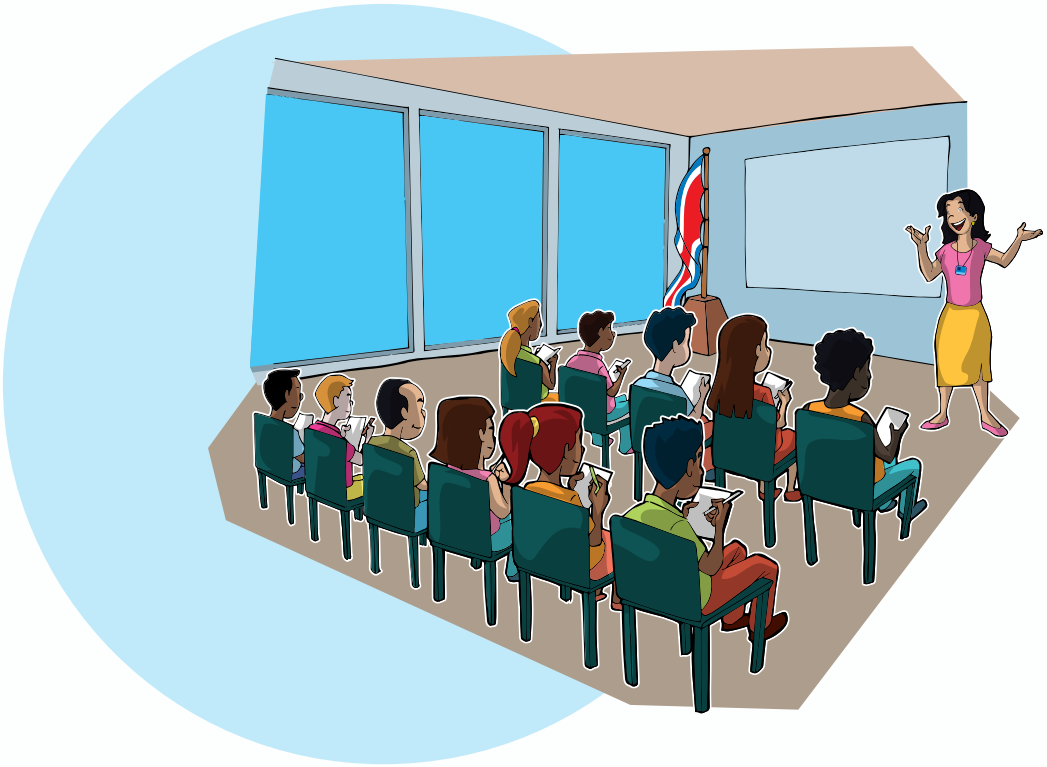
Ley General de Control Interno n.° 8292 del 31 de julio de 2002.

Normas de Control Interno para el Sector Público, emitidas por la Contraloría General de la República. N-2-2009-CO-DFOE.

Directriz R-CO-64-2005 del 01 de julio de 2005 de la Contraloría General de la República.

Circular STSE-0037-2012 del 20 de diciembre de 2012.

Circular STSE-0056-2022 del 30 de agosto de 2022.



4. Matriz de Riesgos

Una matriz de riesgos es una herramienta de control y de gestión normalmente utilizada para identificar las actividades (procedimientos, productos y servicios) más importantes de una institución, el tipo y nivel de riesgos inherentes a estas actividades y los factores internos y externos que generan estos riesgos (factores de riesgo). Igualmente, permite evaluar la efectividad de una adecuada gestión y administración de los riesgos estratégicos, legalidad o cumplimiento, financieros, operativos, tecnológicos, ambientales y otros asociados a liderazgo, ética, cultura organizacional, etc., que impactan la misión de la organización. Debe ser una herramienta flexible que documente los procedimientos y/o procesos. Además, brinda la oportunidad de realizar un diagnóstico objetivo de la situación global de riesgo de una institución y propicia una participación más activa de las unidades operativas y funcionales en la identificación y administración estratégica de los riesgos. Una matriz de riesgos bien diseñada y efectivamente implementada, contribuye a realizar comparaciones objetivas entre proyectos, áreas, productos y servicios, procesos o actividades y se convierte en soporte conceptual y funcional de un efectivo sistema integral de gestión de riesgos. Su fin primordial es brindar información al jerarca para la toma de decisiones oportunas con relación a los riesgos asociados a la gestión diaria.

Igualmente, es necesario que la persona colaboradora en la gestión de riesgos se encuentre capacitada en materia de control interno y comprenda los siguientes términos y definiciones, para el llenado de la matriz de valoración de riesgos.

Las matrices completas del SIVAR se pueden solicitar por medio de correo electrónico: cinterno@tse.go.cr

5. Términos y definiciones

Apetito del riesgo: Se refiere al nivel y tipos de riesgo que una entidad, grupo o conglomerado financiero está dispuesto a asumir, que han sido aprobados por el órgano de dirección, con antelación y dentro de su capacidad de riesgo, para alcanzar sus objetivos estratégicos y plan de negocio. (Acuerdo SUGEF 16-16)

Asumir el riesgo: Después de adoptar las medidas y controles necesarios para mitigar el riesgo, es posible que quede un riesgo residual sin impacto a nivel institucional, el cual se acepta.

Descripción del factor de riesgo: Evento, situación y/o acción que entorpezca el normal desarrollo de las actividades de la institución y que por lo tanto interrumpa el logro de los objetivos. Se refiere, propiamente al riesgo o los riesgos posibles que se presentan en cada una de las actividades del procedimiento.

Nombre de actividad: Actividad sujeta al análisis del riesgo.

Número de actividad: Número de la tarea que forma parte de un procedimiento o número del paso que pertenece a un procedimiento.

O, F, C: Corresponde a las iniciales de operativo, financiero o cumplimiento (legal), respectivamente. Se refieren a la clasificación de los objetivos según su finalidad. Son categorías de objetivos.

Objetivos de cumplimiento: Se plantean con el propósito de acatar y cumplir con las leyes, reglamentos y cualquier otra normativa, tanto interna como externa que regule el campo de acción en que se desenvuelve una organización.

Objetivos de la actividad: Fines que se pretenden lograr cuando se lleva a cabo una actividad. Responden a las preguntas ¿qué se hace, cómo y para qué?

Objetivos financieros: Buscan la manera óptima de control de gastos, reportes, presupuestos y toda la información que incida en los estados financieros.

Objetivos operativos: Persiguen mejorar la manera en que se desarrollan las actividades en la organización. Buscan la eficiencia y eficacia de las operaciones que permiten la generación del producto o servicios que se ofrecen.

Procedimiento: Descripción secuencial de acciones o conjunto de actividades que se deben llevar a cabo para cumplir con un proceso, las cuales se documentan en forma narrativa y secuencial, para cumplir con el objetivo, señalando los responsables y sus roles para ejecutar cada una de estas.

Proceso: Conjunto de procedimientos estructurados y relacionados entre sí, cuya ejecución requiere la interacción de personas y recursos materiales coordinados para conseguir un objetivo previamente establecido. Transforma elementos de entrada (especificaciones, recursos, información, servicios) en resultados (productos y/o servicios). Los resultados de un proceso han de tener un valor añadido respecto a las entradas y pueden constituir directamente elementos de entrada a un siguiente proceso.

Reducir el riesgo: Se deben optimizar los procedimientos y controles.

Riesgo: Probabilidad de que ocurran eventos que tendrían consecuencias sobre el cumplimiento de los objetivos fijados. Los eventos pueden responder a causas internas o externas cuando se relacionan con factores que están fuera de la organización pero tienen alguna incidencia sobre el logro de los objetivos de esta, en caso de llegar a materializarse; lo que pondría de manifiesto la afectación de los servicios que se brindan a la ciudadanía.

Tipos de riesgos: Categorías de riesgos según el impacto de su materialización en el campo de acción en donde se desenvuelve una organización.

Transferir el riesgo: Respaldar y compartir con otra dependencia el riesgo; por ejemplo, las pólizas de seguros.

Unidad administrativa: Unidad u oficina a la que pertenecen las actividades del procedimiento que se analiza.

6. Clasificación de los Riesgos

Los riesgos se clasifican de la siguiente forma:

6.1 Riesgos estratégicos: Se asocian con la forma en que se administra la entidad. Se enfocan en asuntos globales relacionados con el cumplimiento de la misión, visión y los objetivos institucionales, así como con la planificación, organización, coordinación, dirección y control de las actividades de la institución.

Dentro de los riesgos estratégicos se encuentran los siguientes:

6.1.1 Riesgos de la información para la toma de decisiones: Se presentan cuando la información utilizada para respaldar decisiones estratégicas, operacionales y financieras no sea relevante o confiable, o cuando las líneas de acción no sean congruentes con el propósito y estrategias de la organización lo que podría conducir a la toma de decisiones erradas e inconsistentes.

6.1.2 Riesgos de evaluación estratégica: Se asocian a la planificación estratégica que da origen a la misión de la institución, y le permite a esta identificar con claridad sus objetivos y metas en el entorno que la rodea.

6.1.3 Riesgos de imagen: Afectan la percepción del público usuario interno y externo de los servicios y productos de la institución e interfieran en el acercamiento de la ciudadanía con la organización.

6.2 Riesgos de legalidad o cumplimiento: Corresponden a todas aquellas actividades, acciones o hechos que representen un obstáculo para el cumplimiento de las leyes, directrices y cualquier otra normativa que regule el accionar de la institución.

6.3 Riesgos de fraude (corrupción): Corresponden a los hechos o acciones que involucren el uso indebido de la información, materiales, insumos, y demás recursos institucionales en beneficio personal o de unos pocos y en perjuicio de terceros o de recursos públicos, ó que van en contra del ordenamiento jurídico.

Según la Guía para la integración y gestion de riesgos de corrupción en el Sistema específicio de valoración de riesgos (SEVRI), de la Comisión Nacional de Ética y Valores; es necesario identificar las *"áreas de particular sensibilidad y exposición a presentar riesgos de actos contrarios a la integridad o de corrupción"*; asimismo, se citan como ejemplos las relacionadas con los *"recursos humanos", "administración financiera" "contratación administrativa", "transferencia de recursos", "otorgamiento de permisos", "trámites administrativos", "manejo de información confidencial o de uso restringido", "atención de denuncias",* y otros que podrían relacionarse con la misión de la institución. Por esta razón, al momento de identificar los riesgos se debe consultar el portafolio de riesgos de corrupción (ver anexo n.° 1) donde se describen algunos ejemplos de factores de riesgos de corrupción o actos contrarios a la probidad, integridad y ética.

6.4 Riesgos financieros: Son eventos, situaciones o acciones que pudieran entorpecer el normal desarrollo de las actividades que involucren el manejo de recursos financieros públicos y que afecten directamente lo referente al presupuesto institucional. Los hay de dos tipos:

6.4.1 Riesgos presupuestarios: Surgen de la incertidumbre en cuanto a la planeación, asignación y distribución de los recursos que le corresponden a la institución.

6.4.2 Riesgos de la información financiera: Son los relacionados con la planificación, presupuesto e interpretación de la información financiero-contable que se genera en la institución.

6.5 Riesgos operativos: Son los riesgos presentes en las operaciones que se llevan a cabo en la institución producto de las deficiencias en los sistemas de información, en la estructura organizacional o en el desempeño de tareas y en los procesos que conducen a ineficiencias, o bien por el incumplimiento de las políticas o esquemas de trabajo ya establecidos dentro de la institución o de cualquier otra normativa. Los riesgos operativos se clasifican de la siguiente forma:

6.5.1 Riesgos de eficiencia y eficacia de las operaciones: Implican un error en la conducción adecuada de las actividades organizacionales, debido al uso inhapropiado de los recursos disponibles y a la falta de atención de las mejores prácticas que dicten la técnica y el ordenamiento jurídico, lo que impide el logro de los objetivos al menor costo posible.

6.5.2 Riesgos de error: Obedecen a omisiones, confusiones o alteraciones en el ingreso, registro, documentación, transmisión, comunicación o publicación de la información contenida en los sistemas de información o cualquier otro medio utilizado en la institución para administrar toda la información referente a los hechos vitales y actos civiles de la ciudadanía costarricense.

6.5.3 Riesgos de dirección: Implican que quienes ocupen puestos directivos y el resto del personal, no cuenten con la debida dirección, no sepan qué hacer cuando se les presenta un problema, excedan los límites de sus responsabilidades, no reciban motivación, no tengan claras las funciones que deben desempeñar, etc.

6.5.4 Riesgos de seguridad: Se refieren a la pérdida o sustracción de información, documentos, materiales, equipo u otros, necesarios para el cumplimiento de las actividades que coadyuven al logro de los objetivos estratégicos.

6.6 Riesgos tecnológicos: Se centran en la capacidad de la tecnología disponible y proyectada para satisfacer las necesidades y operaciones actuales y futuras de la institución y que, a la vez, sirvan de soporte para el cumplimiento de los objetivos institucionales. Dentro de estos se encuentran los siguientes:

6.6.1 Riesgos de seguridad informática: Son los que presentan los sistemas informáticos en cuanto al acceso a la información administrada a través de médios tecnológicos y su utilización por parte de usuarios internos y externos. Además, del uso indebido o no uso de otros medios que sirvan como respaldo en caso de ser necesario.

6.6.2 Riesgos de equipo tecnológico: Son los que se presentan debido a la obsolescencia, fallas, escasez o mal uso del equipo con que cuenta la institución para el desarrollo de sus actividades ordinarias y extraordinarias.

La gestión de riesgos tecnológicos debe responder a las amenazas que puedan afectar el logro de los objetivos de la institución, debe estar integrada al SIVAR considerando el marco de gestión de riesgo tecnológico aplicable, como por ejemplo: las *"Normas técnicas para la gestión y el control de las tecnologías de información",* las cuales se encuentran estructuradas de la siguiente forma:

- Marco de Gobierno y Gestión de las Tecnologías de Información.
- Documento de Portafolio de Riesgos (Puede ser utilizado para identificar y registrar riesgos en el SIVAR (ver anexo n.° 2)
- Matriz de Guía de Implementación; y
- Perfil de la Gestión de Tecnologías de la Información.

Esta norma técnica emitida por el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT) fue aprobada por el CDIR, en la sesión ordinaria n.°59-2021, celebrada el 14 de diciembre de 2021 y comunicada mediante oficio CDIR-503-2021 de misma fecha; *"como marco regulador que guíe al Tribunal en materia de tecnologías de información."*

6.7 Riesgos ambientales: Se presentan por factores ambientales como la humedad, el polvo, desastres naturales (inundaciones, terremotos, huracanes), plagas, entre otros; que pueden afectar los recursos de la institución, también incluye la respuesta ante desastres y crisis.

7. Otros Riesgos

Son los riesgos que no se encuentran contemplados en las actividades descritas en el procedimiento, pero que se identifican como un riesgo potencial, sea por una situación interna o externa. Estos se incluirán al final de las actividades del procedimiento de la matriz de riesgos con la inscripción *"otros riesgos"* y en la casilla de "n.° de actividad" se consigna N/A. Por ejemplo: riesgos asociados al liderazgo, a la cultura organizacional, a comportamientos o principios éticos de las personas colaboradoras, calidad de los servicios, riesgos externos asociados a cambios en el entorno, o a alguna situación especial como la pandemia de COVID-19, incendios, etc.

8. Valoración del Riesgo

Es el segundo componente del Sistema de Control Interno. La Ley General de Control Interno, en su artículo 2, inciso f), la define como: *"identificación y análisis de los riesgos que enfrenta una institución, tanto de fuentes internas como externas relevantes para la consecución de los objetivos; deben ser realizados por el jerarca y los titulares subordinados, con el fin de determinar cómo se deben administrar dichos riesgos."*

Uno de los objetivos del SIVAR es producir información para la toma de decisiones, de tal manera que la institución se mantenga en un nivel de riesgo aceptable, y se logren los objetivos institucionales. Sobre la valoración de riesgo, es importante tener presente lo que establece la Ley General de Control Interno en su artículo 14:

> *Artículo 14.- **Valoración del riesgo.** En relación con la valoración del riesgo, serán deberes del jerarca y los titulares subordinados, entre otros, los siguientes:*
>
> *a) Identificar y analizar los riesgos relevantes asociados al logro de los objetivos y las metas institucionales, definidos tanto en los planes anuales operativos como en los planes de mediano y de largo plazos.*
>
> *b) Analizar el efecto posible de los riesgos identificados, su importancia y la probabilidad de que ocurran, y decidir las acciones que se tomarán para administrarlos.*
>
> *c) Adoptar las medidas necesarias para el funcionamiento adecuado del sistema de valoración del riesgo y para ubicarse por lo menos en un nivel de riesgo organizacional aceptable.*
>
> *d)Establecer los mecanismos operativos que minimicen el riesgo en las acciones por ejecutar.*

Asimismo, se debe considerar lo establecido en la Norma 3.3 de Control Interno para el Sector Público:

3.3 Vinculación con la planificación institucional.

> *La valoración del riesgo debe sustentarse en un proceso de planificación que considere la misión y la visión institucionales, así como objetivos, metas, políticas e indicadores de desempeño claros, medibles, realistas y aplicables, establecidos con base en un conocimiento adecuado del ambiente interno y externo en que la institución desarrolla sus operaciones y en consecuencia, de los riesgos correspondientes.*

Asimismo, los resultados de la valoración del riesgo deben ser insumos para retroalimentar ese proceso de planificación, aportando elementos para que el jerarca y los titulares subordinados, estén en capacidad de revisar, evaluar y ajustar periódicamente los enunciados y supuestos que sustentan los procesos de planificación estratégica y operativa institucional, para determinar su validez ante la dinámica del entorno y de los riesgos internos y externos.

Por lo anterior, es importante recalcar que, al momento de realizar el análisis del riesgo, es preciso considerar la vinculación de la actividad con los objetivos formulados en los planes estratégico, táctico y operativo. Así las cosas, se deben tomar en cuenta los ejes y objetivos estratégicos del Plan Estratégico Institucional, así como las líneas de acción, para determinar los riesgos estratégicos, de manera que se puedan asociar ya sea al objetivo estratégico 1, 2 o 3 del PEI. (Ver tabla 1)

Tabla n.°1.
Objetivos estratégicos del PEI

Eje	Objetivo Estratégico
I. Organización y arbitraje de procesos electorales	1. Robustecer la integridad de las contiendas electorales por medio del fortalecimiento al acceso a los recursos por parte de los partidos políticos, así como de la promoción de la participación electoral informada e inclusiva de la ciudadanía en esas contiendas.
II. Servicios de registración civil e identificación de personas	2. Fortalecer la prestación de los servicios registrales, de naturalización e identificación a todos los ciudadanos, en especial de la población en situación de vulnerabilidad, mediante la implementación de iniciativas que amplíen su cobertura y su accesibilidad.
III. Formación en democracia	3. Promocionar la cultura democrática en la ciudadanía, mediante el fortalecimiento de las acciones orientadas al fomento de la cultura cívica, para el ejercicio responsable de los derechos político-electorales.

Fuente: Plan Estratégico Institucional PEI 2019-2024

9. Identificación del Riesgo

Para la identificación del riesgo, es importante determinar y describir los eventos tanto internos como externos que puedan afectar de manera significativa el cumplimiento de los objetivos. Esta identificación puede realizarse por áreas, actividades, tareas o procesos, de acuerdo con lo que defina la institución. Debe llevarse a cabo de forma

continua y exhaustiva, y abarcar todos los niveles de la organización, considerando también, posibles riesgos de "fraude o corrupción", de tal manera que se asegure la identificación de todos los riesgos (ver portafolios de algunos riesgos en los anexos 1 y 2). La identificación del riesgo debe ser efectuada por las personas funcionarias responsables de la unidad administrativa, quienes son los especialistas y conocen los riesgos a los que se enfrentan. Se debe considerar las siguientes interrogantes: **¿Qué puede suceder?, ¿cómo puede suceder? y ¿por qué puede suceder?** (Ver figura 1)

Figura 1

Identificación de los riesgos			
Considerar los eventos que podrían afectar de forma significativa el cumplimiento de los objetivos institucionales. Estos deberán organizarse de acuerdo con la estructura de riesgos institucional.	Las posibles causas, internas y externas, de los eventos identificados y las posibles consecuencias de la ocurrencia de dichos eventos sobre el cumplimiento de los objetivos.	Las formas de ocurrencia de dichos eventos y el momento y lugar en el que podrían ocurrir.	Las medidas para la administración de riesgos existentes que se asocian con los riesgos identificados.

Fuente: Elaboración propia con base en información del Curso de Control Interno de la CGR, Componente 2 Valoración de Riesgo

10. Análisis del Riesgo

Se realiza considerando el nivel de impacto y la probabilidad de ocurrencia del factor de riesgo, para determinar el nivel de exposición al riesgo, ya sea bajo, medio o alto, de esta forma se establecen acciones preventivas o correctivas, a fin de evitar la materialización del riesgo o mitigarlo. Sobre el nivel de exposición al riesgo se cuenta con los siguientes indicadores:

- **Indicador de riesgos:** Es una métrica que suministra información sobre el nivel de exposición a un riesgo específico en la organización, en un momento dado. Al analizarlo muestra de forma temprana la aparición de riesgos. Mide la cantidad de veces que se puede materializar el factor de riesgo.

- **Impacto:** Consecuencias que puede ocasionar a la institución la materialización del riesgo. Se mide en términos cuantitativos a través de indicadores o de criterio subjetivo según una escala; para el SIVAR se utiliza la escala de nivel de impacto mostrada en la tabla 2:

Tabla n.°2
Niveles de impacto

Puntuación	Definición del Impacto	Nivel
5	Impacto bajo: Si el hecho llegara a presentarse tendría bajo impacto sobre la gestión institucional	Bajo (Verde)
10	Impacto medio: Si el hecho llegara a presentarse tendría un impacto o efecto medio en la gestion institucional.	Medio (Amarillo)
15	Impacto alto: Si el hecho llegara a presentarse tendría alto impacto o efecto en la gestión de la Institución.	Alto (Rojo)

Fuente: Plan Estratégico Institucional PEI 2019-2024

Probabilidad: Se entiende como la posibilidad de ocurrencia del riesgo. Puede ser medida con criterios de frecuencia o teniendo en cuenta la frecuencia de factores internos y externos que pueden propiciar el riesgo aunque no se haya presentado nunca; tomando en consideración los criterios que se muestran en la tabla 3:

Tabla n.°3
Niveles de probabilidad

Puntuación	Probabilidad de ocurrencia	Nivel
5	Es poco probable que el hecho se presente	Bajo (Verde)
10	Es probable que el hecho se presente	Medio (Amarillo)
15	Es muy probable que el hecho se presente	Alto (Rojo)

Fuente: Elaboración propia Unidad de Control Interno (2022)

Además es importante tener claros los siguientes términos de aplicación:

Riesgo inherente: es el que por su naturaleza no puede separarse de la actividad donde se presenta, es decir, es propio de esta.

Calificación de riesgo inherente. Se obtiene al realizar la siguiente fórmula matemática:

impacto x probabilidad = calificación de riesgo inherente

Nivel de riesgo: Grado de exposición al riesgo que se determina a partir del análisis de la probabilidad de ocurrencia del evento y de la magnitud de su consecuencia potencial sobre el cumplimiento de los objetivos fijados, permite establecer la importancia relativa del riesgo.

Nivel del riesgo inherente: indica si el nivel es bajo, medio o alto, con el siguiente código de colores: verde (bajo), amarillo (medio), rojo (alto).

11. Actividades de Control

Las actividades de control corresponden a las acciones que se llevan a cabo para realizar las tareas respectivas de cada procedimiento con lo que se asegura razonablemente la operación, el fortalecimiento del SCI y el logro de los objetivos institucionales. Dichas actividades deben ser dinámicas, de modo que se puedan realizar mejoras; no están descritas dentro de las actividades del procedimiento, pero una vez establecidas deben incluirse.

El ámbito de aplicación está referido a todos los niveles y funciones de la institución. De acuerdo con lo dispuesto en las Normas de control interno para el Sector Público, específicamente la 4.1 señala entre otras cosas:

> *(…) la gestión y la operación del SCI deben contemplar, de acuerdo con los niveles de complejidad y riesgo involucrados, actividades de control de naturaleza previa, concomitante, posterior o una conjunción de ellas. Lo anterior debe hacer posible la prevención, la detección y la corrección ante debilidades del SCI y respeto de los objetivos, así como ante indicios de la eventual materialización de un riesgo relevante.*

Requisitos de las actividades de control según la Norma 4.2 de control interno para el Sector Público:

> *Las actividades de control deben reunir los siguientes requisitos:*
>
> ***a. Integración a la gestión.*** *Las actividades de control diseñadas deben ser parte inherente de la gestión institucional, e incorporarse en ella en forma natural y sin provocar menoscabo a la observancia de los principios constitucionales de eficacia, eficiencia, simplicidad y celeridad, y evitando restricciones, requisitos y trámites que dificulten el disfrute de los derechos fundamentales de los ciudadanos.*
>
> ***b. Respuesta a riesgos****. Las actividades de control deben ser congruentes con los riesgos que se pretenden administrar, lo que conlleva su dinamismo de acuerdo con el comportamiento de esos riesgos.*
>
> ***c. Contribución al logro de los objetivos con un costo razonable.*** *Las actividades de control deben presentar una relación satisfactoria de costo-beneficio, de manera que su contribución esperada al logro de los objetivos, sea mayor que los costos requeridos para su operación.*
>
> ***d. Viabilidad.*** *Las actividades de control deben adaptarse a la capacidad de la institución de implantarlas, teniendo presente, fundamentalmente la disponibilidad de recursos, la capacidad del personal para ejecutarlas correcta y oportunamente, y su ajuste al bloque de legalidad.*
>
> ***e. Documentación.*** *Las actividades de control deben documentarse mediante su incorporación en los manuales de procedimientos, en las descripciones de puestos y procesos, o en documentos de naturaleza similar. Esa documentación debe estar disponible, en forma ordenada conforme a criterios previamente establecidos, para su uso, consulta y evaluación.*

f. Divulgación. *Las actividades de control deben ser de conocimiento general, y comunicarse a los funcionarios que deben aplicarlas en el desempeño de sus cargos. Dicha comunicación debe darse preferiblemente por escrito, en términos claros y específicos.*

Según la Guía técnica para el desarrollo de auditorías de la ética, de la Contraloría General de la República, se debe integrar la ética a los sistemas de gestión, de tal manera que se establezcan controles en los sistemas y procedimientos utilizados en las áreas de especial sensibilidad y de exposición a esos riesgos. Dicha guía cita como ejemplo las siguientes áreas para el establecimiento de controles en materia de ética:

- ***Recursos humanos*** *(reclutamiento, selección, promoción, compensación y otros incentivos). Esta área tiene una importancia fundamental, por cuanto incide directamente en las capacidades de los integrantes de la organización, para contribuir a un clima ético positivo. Debe preverse la aplicación de procedimientos para garantizar que el recurso humano posea los perfiles idóneos, y que su administración observe y promueva la aplicación de los principios y valores éticos que rigen la gestión organizacional.*

- ***Administración financiera*** *(percepción y disposición de fondos). En virtud de la vulnerabilidad de los activos involucrados, requiere de controles formales que sean aplicados por personal caracterizado por altos principios y valores éticos.*

- ***Contratación administrativa.*** *Debe conducirse con transparencia e igualdad, otorgando los mismos derechos y obligaciones a todos los oferentes, y así deben garantizarlo los procedimientos establecidos en la institución.*

- ***Transferencia de recursos.*** *El manejo de los recursos transferidos debe ajustarse a los fines previstos, para lo cual deben propiciarse los mecanismos atinentes.*

- ***Otorgamiento de permisos.*** *Por un lado, debe garantizarse que los funcionarios encargados de conceder los permisos no hagan uso indebido de sus facultades. Por otro, debe vigilarse que el permiso sea utilizado correctamente por quien lo ha recibido.*

- ***Trámites administrativos.*** *Independientemente del solicitante, debe atenderse de manera efectiva y oportuna, previniendo cualquier intento de soborno u otra conducta antiética.*

- ***Manejo de información confidencial o de uso restringido.*** *Deben tenerse presentes las limitaciones establecidas constitucional y legalmente para el manejo de información, de manera que se evite su suministro o difusión irregular.*

- ***Actividades en las que se da una alta injerencia política.*** *En la gestión diaria de la organización, se debe evitar el abuso de facultades e injerencias políticas que sean contrarias a los principios y valores éticos institucionales.*

• ***Atención de denuncias*** *y comunicaciones sobre eventuales conductas antiéticas y conflictos de intereses. Especialmente en las operaciones sensibles, debe garantizarse la posibilidad de denunciar, así como el manejo confidencial del caso y la atención correcta, consistente y oportuna de lo comunicado, independientemente de los supuestos infractores.*

• ***Otros*** *relevantes de acuerdo con la actividad de la organización y del nivel de riesgo que conllevan. (La negrita no es del original).*

12. Control

Tipo de control: Corresponde a la clasificación de los controles según su naturaleza, puede ser control preventivo (P), control detectivo (D) y control correctivo (C):

- **Control preventivo:** Se aplica con el propósito de prever o evitar la ejecución de acciones que originen algún riesgo.
- **Control detectivo:** Se emplea con el propósito de detectar las actividades que originan o podrían originar algún riesgo para aplicar las medidas o acciones pertinentes en procura de la minimización de la probabilidad de ocurrencia.
- **Control correctivo:** Se usa para corregir y mejorar las acciones en procura de bajar el nivel de riesgo.

Alcance del control (S; I): Se refiere a la efectividad del control aplicado el cual puede ser suficiente (S) o insuficiente (I).

- **Control suficiente:** Su alcance es eficiente en cuanto a la minimización de los riesgos y de su efecto, en caso de que se materialicen.
- **Control insuficiente:** Su alcance no es eficiente en cuanto a la minimización de los riesgos y de su efecto en caso de que se materialicen, a pesar de que se aplica.

Calificación del control: Puntaje que se aplica al control sea este suficiente o insuficiente; el valor de la calificación varía dependiendo del rango de valores.

13. Calificación del Riesgo

Continuando con la calificación del riesgo, es importante conocer cómo se define:

Calificación de riesgo residual: Cuota de riesgo que es imposible eliminar luego de haber aplicado los controles. Se obtiene mediante la siguiente fórmula matemática:

calificación del riesgo inherente - calificación del control = calificación del riesgo residual.

Nivel de riesgo residual: Indica si el nivel es bajo, medio o alto, con el siguiente código de colores: verde (bajo), amarillo (medio), rojo (alto) respectivamente.

Niveles de riesgo alto, medio o bajo:

- **Nivel de riesgo alto** (identificados con el color rojo) pretende priorizar todas las actividades de control posibles dentro de la organización, teniendo en cuenta el análisis costo-beneficio. Muchas veces implementar unas medidas de control pueden suponer un costo mayor que el beneficio que puede reportar. Este análisis permite cuantificar si compensa o no adoptar las actividades de control.
- **Nivel de riesgo medio** (identificados con el color amarillo) pretende evaluar y ejercer supervisión de controles claves y relevantes. De manera que con las actividades de control implementadas se pueda pasar al nivel de riesgo bajo.
- **Nivel de riesgo bajo** (identificados con el color verde) se aplicará a todas las actividades en las que los riesgos identificados no causan un impacto significativo o relevante y podrán ser asumidos por la administración. No se necesita implementar acciones correctivas al tratarse de un riesgo del día a día caracterizado por la propia actividad de la unidad administrativa; por lo tanto, las actividades de control son suficientes para evitar o mitigar su materialización; lo que no generará un alto impacto para la consecución de los objetivos.

Escala de calificación del riesgo: Se utiliza para medir el riesgo inherente y el riesgo residual (ver figura 2).

Figura 2
Escala de calificación del riesgo

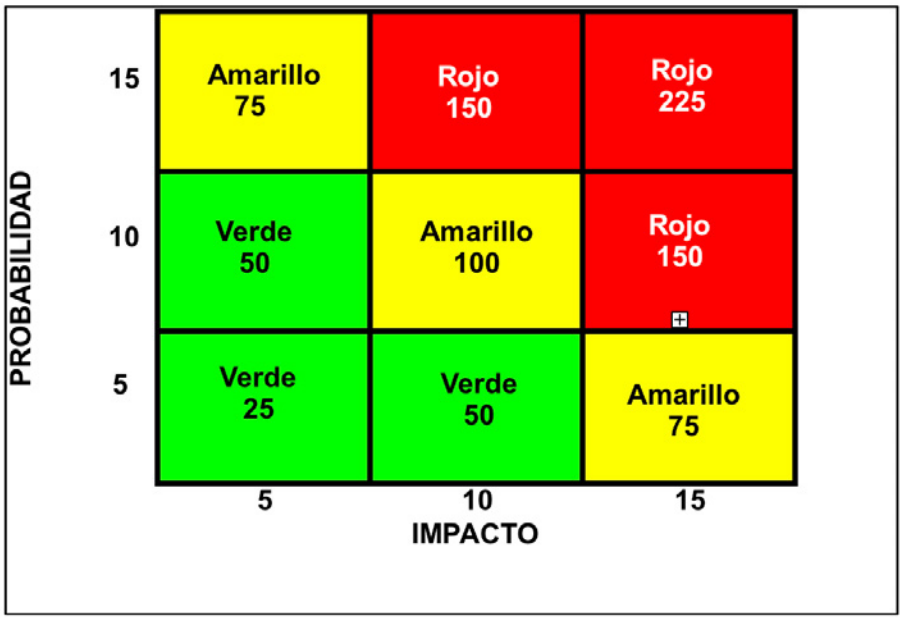
• **Riesgo bajo:** De cero a menos de setenta y cinco

• **Riesgo medio:** De setenta y cinco a menos de ciento cincuenta

• **Riesgo alto:** De ciento cincuenta a doscientos veinticinco inclusive

La anterior escala se obtiene con base en todas las posibles opciones que surgen al multiplicar **impacto por probabilidad,** como se muestra en el Mapa de riesgos inherente (figura 3)

Figura 3
Mapa de riesgos inherente



14. Acciones Preventivas o Correctivas

Las acciones preventivas o correctivas se plantean con la finalidad de fortalecer los controles y la aplicación concreta de las opciones del manejo de los riesgos relevantes (evitar, aceptar, reducir, transferir, compartir), que entrarán a prevenir o a reducir el riesgo: *"Cuando el funcionario competente detecte alguna deficiencia o desviación en la gestión o en el control interno, o sea informado de ella, debe emprender oportunamente las acciones preventivas o correctivas pertinentes para fortalecer el SCI de conformidad con los objetivos y Recursos institucionales" (NCISP,2009, p.27).*

La acción siempre debe ir enfocada a la causa del riesgo, según los objetivos y recursos institucionales, y debe dar

prioridad al tratamiento de los riesgos de alto impacto. Esta acción debe ser verificable, medible y responder a las siguientes preguntas: ***"Qué se va hacer, cómo, para qué y cuando".***

Estado de la acción: Se encuentra en concordancia con el nivel de avance en la implementación de la acción preventiva o correctiva, a saber: pendiente, en proceso o concluida.

Grado de avance: Corresponde al porcentaje que se asigna, según el avance o el estado en que se encuentra la acción para su implementación, ya sea pendiente (0%), en proceso (1% - 99%) o concluida (100%). Además, se debe indicar y aportar la evidencia del cumplimiento. Lo anterior, obedece a una recomendación planteada por la Auditoría Interna. Al respecto, es importante señalar que la acción preventiva o correctiva debe quedar implementada en el periodo (un año).

15. Mapas de Riesgos

Mapa de riesgos del procedimiento.

Se compone de una tabla resumen con la calificación del riesgo inherente, la calificación del control, la calificación residual, y el nivel de riesgo residual del procedimiento; que recopila de la información contenida en la matriz de valoración de riesgos y se genera automáticamente.
En el mapa de riesgo residual del procedimiento, debe ubicarse manualmente, el número de la actividad del procedimiento de acuerdo con la nota de calificación de riesgo residual.

Mapa de riesgos global

Está compuesto por la **tabla de riesgo global** de la unidad administrativa, (esta tabla se completa en forma automática, con la calificación de riesgo residual obtenida en cada uno de los procedimientos). En el mapa global se debe ubicar manualmente el código de cada procedimiento de acuerdo con la calificación del riesgo residual obtenida y con los niveles del mapa de colores. Es importante mencionar que, este mapa se debe completar una vez realizada la valoración de todos los riesgos, y debe recopilar la totalidad de los procedimientos de la oficina.

16. Plan de Acción

El plan de acción contribuye a la mitigación de los riesgos con alto o medio impacto, indica cuáles acciones correctivas se deben emprender, el plazo y la persona responsable de realizarlas. Al completar las casillas en la matriz de riesgos, el plan de acción **se consolida automáticamente.** Importante recalcar, que la acción debe quedar implementada dentro del período (un año). Las acciones correctivas concluidas deberán registrarse en el manual de procedimientos, en caso de que sean reiterativas para mejorar el control; las pendientes y en proceso se mantendrán en el plan de acción donde se justificará con evidencias su incumplimiento.

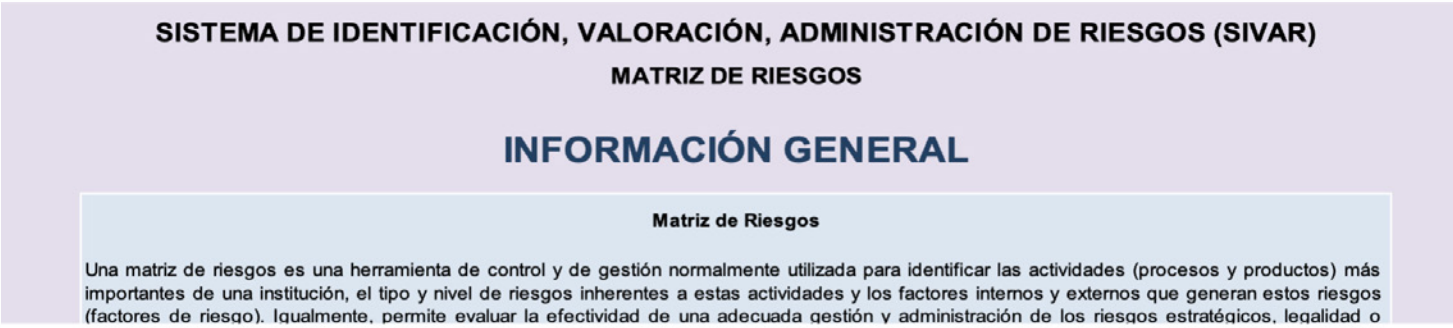
17. Matriz de Riesgos

La matriz de riesgos es un documento en excell está conformado por diferentes pestañas numeradas y tituladas, según el siguiente detalle:

1. Información general (pestaña1)

Se refiere a la información general que contiene la matriz de riesgos, el marco de aplicación y su estructura (ver figura 4).

Figura 4
Información General



2. Instrucciones para completar la matriz de valoración de riesgos SIVAR. (pestaña 2)

En este apartado se muestran las instrucciones en forma detallada para la valoración de riesgos de cada uno de los procedimientos de la unidad administrativa, así como de otros riesgos internos o externos que no se encuentran asociados a los procedimientos.

Figura 5
Instrucciones

Instrucciones para completar la matriz de valoración de riesgos SIVAR

1. **Información General** (Pestaña n.°1) Se refiere a la información general que contiene la matriz de riesgos, el marco de aplicación y su estructura, se recomienda su lectura.

Ilustración n.°1. Información contenida en la pestaña n.°1.

SISTEMA DE IDENTIFICACIÓN, VALORACIÓN, ADMINISTRACIÓN DE RIESGOS (SIVAR)
MATRIZ DE RIESGOS

3. Detalle de los procedimientos.(pestaña 3)

Figura 6
Detalle de las actividades de los procedimientos.

TRIBUNAL SUPREMO DE ELECCIONES		
SISTEMA DE IDENTIFICACIÓN Y VALORACIÓN DE RIESGOS (SIVAR)		
NOMBRE DE LA DIRECCIÓN	Dirección Ejecutiva	
Nombre de la Unidad Administrativa	Unidad de Control Interno	
Instrucciones: En este apartado deben consignarse el código y nombre del procedimiento así como todas las actividades de cada		
No. Actividad	(Código)	(Código)
	(Nombre del Procedimiento 1)	(Nombre del Procedimiento 2)
	Nombre de la Actividad	Nombre de la Actividad
1		
2		

- Nombre de la dirección a la cual pertenece la unidad administrativa.
- Nombre de la unidad administrativa a la que corresponden los procedimientos.

Además, es necesario consignar **el código y nombre del procedimiento** y todas las actividades de cada uno de los procedimientos de la unidad administrativa; esta información se cargará automáticamente en las pestañas siguientes del punto 4, para proceder con la valoración de cada uno de los riesgos, tal como se aprecia en la figura 6.

4. SIGLAS-P00X. Código del procedimiento . (Pestaña 4)

Contiene toda la información para proceder con la valoración de los riesgos, para lo cual es preciso completar lo solicitado. (la información de esta página, se despliega en forma vertical); ver figura 7.

Figura 7
SIGLAS-P00X Información contenida en la pestaña 4.

TRIBUNAL SUPREMO DE ELECCIONES		
SISTEMA DE IDENTIFICACIÓN Y VALORACIÓN DE RIESGOS (SIVAR)		
	NOMBRE DE LA DIRECCIÓN	Dirección Ejecutiva
	Nombre de la Unidad Administrativa	Unidad de Control Interno
Instrucciones: En este apartado deben consignarse el código y nombre del procedimiento así como todas las actividades de cada		
No. Actividad	(Código)	(Código)
	(Nombre del Procedimiento 1)	(Nombre del Procedimiento 2)
	Nombre de la Actividad	Nombre de la Actividad
1		
2		

• **Número de la actividad:** a la cual está sujeto el análisis del riesgo; se encuentra registrado en la matriz.

• **Descripción de la actividad:** se despliega automáticamente con la información que se completa en la pestaña 3.

• **Objetivo de la actividad:** anotar en la casilla el "objetivo de la actividad", según corresponda, de acuerdo con la clasificación respectiva, sea objetivo estratégico, operativo, financiero o de cumplimiento (legal).

Valoración del riesgo.

a) Identificación del Riesgo.

- **Describir el ó los factor(es) de riesgo:** corresponde propiamente al posible riesgo que se presenta en cada una de las actividades que se realizan, que entorpezca el normal desarrollo de las actividades. Considerar los siguientes criterios **causa** (generadora del riesgo) – **efecto** (forma como puede materializarse el riesgo, lo que implica). Ej: Debido a que no hay un control de documentos, no hay trazabilidad de la correspondencia lo que implica que los documentos se puedan extraviar.

Cabe mencionar que, según circular DE-0029-2016, se debe realizar la valoración de los riesgos a todas las actividades del procedimiento. Por tal razón, se debe identificar y definir el factor de riesgo ó indicar: *"Se realizó la valoración de riesgos y no se identificaron riesgos asociados a esta actividad del procedimiento". De este modo se justifica el resto de casillas de la misma actividad que quedan en blanco.*

b) Análisis del riesgo

Figura 8
Valoración del riesgo

Análisis del riesgo					
TIPO RIESGO	Legalidad o cumplimiento	IMPACTO		PROBABILIDAD	
INDICADOR					
Calificación del Riesgo Inherente	0			Nivel de Riesgo Inherente	0
Actividad de Control		Tipo de Control			
Describir la actividad de control para mitigar el riesgo.					
Alcance del control				Calificación del control	0
Calificación del Riesgo Residual	0			Nivel de Riesgo Residual	0

- **Tipo de riesgo:** seleccionar en esta casilla la categoría correspondiente. Si el riesgo está asociado a alguno ***de los objetivos estratégicos, legalidad o cumplimiento, financiero, operativo, tecnológico, o ambienta***l o si se encuentra asociado a otros riesgos como ***al liderazgo, a la cultura organizacional, a comportamientos éticos de los colaboradores, a la calidad de los servicios,*** tal como se describe en el apartado n.° 7 de "Otros riesgos".

Para alinear los riesgos a los objetivos estratégicos, se debe identificar para cada actividad su relación directa con los objetivos estratégicos de la institución, así como el grado de afectación en el cumplimiento de estos.

- **Impacto:** en esta casilla se debe seleccionar el puntaje que considera puede tener o tiene el riesgo identificado si se materializa, según la escala que se muestra en la figura 9:

Figura 9
Escala de nivel de impacto.

Bajo	5		(Verde)
Medio	10		(Amarillo)
Alto	15		(Rojo)

Fuente: Elaboración propia Unidad de Control Interno (2022) con base en el Modelo Metodológico SIVAR.

El impacto corresponde a las consecuencias que puede ocasionar la materialización del o los factor (es) de riesgo, en el cumplimiento de los objetivos de la unidad administrativa. Se mide en términos cuantitativos a través de indicadores o de criterio subjetivo.

- **Probabilidad:** anotar la puntuación que se estime puede tener o tiene el riesgo identificado ante la probabilidad de ocurrencia, según la escala:

Figura 10
Escala sobre probabilidad de ocurrencia.

Bajo	5		(Verde)
Medio	10		(Amarillo)
Alto	15		(Rojo)

Fuente: Elaboración propia Unidad de Control Interno (2022) con base en el Modelo Metodológico SIVAR.

La probabilidad se puede medir con criterios de frecuencia (repetición) o teniendo en cuenta la frecuencia de factores internos y externos que pueden propiciar el riesgo, aunque no se haya presentado nunca.

- **Indicador:** en esta casilla se debe definir la información cuantitativa en términos de **"cantidad de veces"** que podría llegar a materializarse el factor de riesgo en un período determinado, sea por día, mes, semana, año, etc. **Se refiere a un indicador de riesgos, no consignar fórmulas, ni indicadores de cumplimiento.**

- **Calificación de riesgo inherente:** en esta casilla se refleja automáticamente el resultado de multiplicar (impacto x probabilidad = nivel de riesgo inherente), indicándose con el color respectivo, según corresponda el nivel de riesgo: alto (rojo), medio (amarillo), bajo (verde) así como el nivel de riesgo inherente.

Control

- **Actividad de control:** en la casilla se describen las acciones que se llevan a cabo con el fin de mitigar el impacto y probabilidad de ocurrencia del factor de riesgo.

- **Tipo de control:** seleccionar de acuerdo con la clasificación de los controles: P=preventivo, D=detectivo o C=correctivo, según corresponda.

- **Alcance del control:** (S;I) respecto a la efectividad del control aplicado, debe seleccionarse una opción, a saber: Suficiente (S) o Insuficiente (I).

- **Calificación del Control:** en esta casilla aparecen los valores resultantes (automáticamente), una vez definido el alcance del control (S: suficiente , I: insuficiente).

- **Nivel de riesgo residual promedio:** se genera automáticamente por medio de la sumatoria de todos los valores de la calificación del riesgo residual para obtener el promedio total ya sea bajo, medio o alto.

Seguidamente en la figura 11 se muestra la ponderación para la calificación del control si es suficiente o insuficiente, según el nivel de riesgo inherente:

Figura 11
Calificación de control

Condición	Calificación
Si el riesgo inherente es alto y el control es suficiente	125
Si el riesgo inherente es alto y el control es insuficiente	75
Si el riesgo inherente es medio y el control suficiente	70
Si el riesgo inherente es medio y el control insuficiente	50
Si el riesgo inherente es bajo y control suficiente	20
Si el riesgo inherente es bajo y el control insuficiente	5

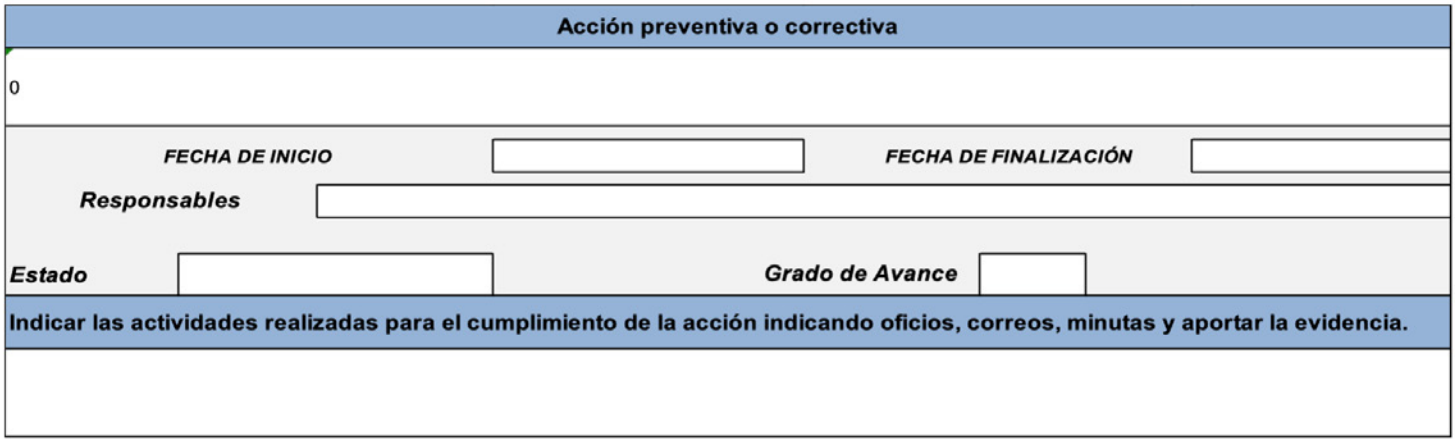
Fuente: Elaboración propia Unidad de Control Interno(2022) con base en la Guía del SIVAR 2017

Se aclara que, si el riesgo inherente es medio, con la calificación de control suficiente en 70 queda una calificación de riesgo residual de 5 esto debido a que siempre existe un riesgo inherente a pesar de que el control sea suficiente. Igualmente, si la calificación del riesgo inherente mínima es de 25 el cual se obtiene al multiplicar impacto x probabilidad de ocurrencia, la calificación de control suficiente será de 20, de tal manera que la calificación del riesgo residual sea de 5.

Acción preventiva o correctiva

En esta casilla se anota la acción que se podría implementar -que resulte viable- para controlar o mitigar los riesgos relevantes identificados en las actividades del procedimiento, en caso de que existieran. Si la actividad de control es suficiente para mitigar el riesgo debe indicarse: *"No se propone acción correctiva, dado que con la actividad de control es suficiente para mitigar el riesgo."* Indicar si la acción es preventiva o correctiva.

Figura 12
Acción preventiva o correctiva



- **Estado:** anotar la condición en que se encuentra la acción correctiva, en concordancia con el nivel de avance del cumplimiento de la acción, a saber:

o Pendiente: no se ha realizado ninguna gestión.

o En proceso: se han realizado algunas gestiones, pero no son suficientes para dar por implementada la acción correctiva.

o Concluida: se realizaron las gestiones necesarias y la acción correctiva se encuentra implementada.

Deberán indicarse las actividades realizadas para el cumplimiento de la acción preventiva **o** correctiva, así como evidenciarlas mediante correos electrónicos, oficios, minutas, etc., los cuales deberán aportarse cuando se presenta la matriz. Cabe mencionar, que la unidad administrativa cuenta con un año para concluir e implementar la acción correctiva.

- **Grado de avance:** completar esta casilla según el grado de cumplimiento de la acción correctiva, en concordancia con cada uno de los estados, a saber:

Pendiente (0%)

En proceso (1% - 99%)

Concluida (100%)

Además, indicar las fechas de inicio y finalización de la acción (fecha en que se implementa) así como los responsables de llevarlas a cabo.

Por otra parte, para llevar el registro de las actividades es necesario que la unidad administrativa, complete la casilla dispuesta para ese fin. La del total de riesgos y acciones preventivas o correctivas se completan en forma automática.

Figura 13
Información sobre la totalidad de los riesgos

Cantidad de actividades, riesgos y acciones que se identifican en el procedimiento:				
Total de actividades	*Total de Riesgos*	*Total de acciones preventivas o correctivas:*		
		Pendientes	*En Proceso*	*Concluidas*
	0	*0*	*0*	*0*
"Se realizó la valoración de riesgos de todas las actividades que componen el procedimiento, y se determinó que el nivel de riesgo residual, de la actividad o actividades será asumido por la oficina". Lo anterior, según lo dispuesto en Circulares DE-029-2016 del 25 de agosto de 2016 y DE-012-2018 del 03 de abril de 2018.				
Anotar el número de la actividad o actividades a las que no se propone acción preventiva o correctiva:				

Al finalizar el llenado de la matriz anotar el nombre y apellidos de quien la elaboró, revisó, aprobó, firma y fecha. Debe remitirse también en formato pdf, firmado por el jefe de la unidad administrativa.

- **Mapa de riesgos de los procedimientos:** se realiza con la información obtenida en la Tabla resumen de riesgos del procedimiento, que se genera automáticamente a partir de los valores indicados en el análisis y el mapa de riesgos propiamente. (ver ejemplos en tabla 4 , y figuras 14 y 15).

Tabla n.°4
Resumen de riesgos del procedimiento

Código del Procedimiento DE-P001-v01			
No. Actividad	**Calificación inherente**	**Calificación del control**	**Calificación residual**
1	50	25	25
2	75	25	50
3	100	50	50
4			
5			
Nivel de riesgo inherente)	75	Nivel de riesgo residual	41,66

Fuente: Elaboración propia Unidad de Control Interno (2022) Con base en el Modelo Metodológico SIVAR.

***Los valores de las columnas se promedian, al aplicar la fórmula: calificacion de riesgo inherente - calificación de riego residual = a nivel de riesgo residual.**

Figura 14
Mapa de riesgo inherente

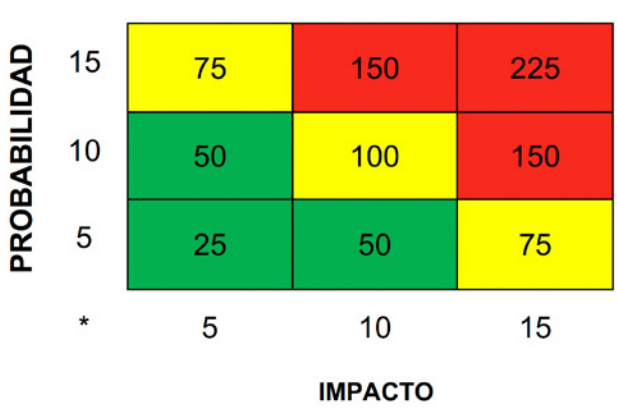
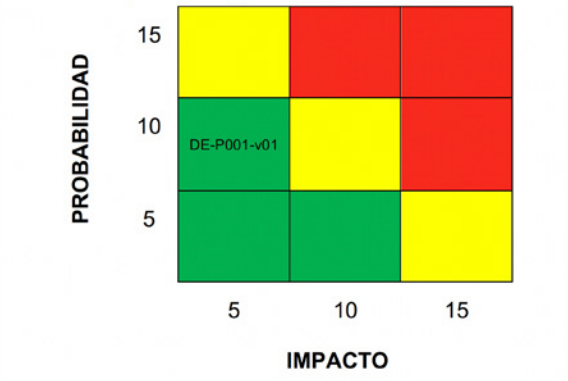


Figura 15
Mapa de riesgo residual

Medio	Alto	Alto
Bajo	Medio	Alto
Bajo	Bajo	Medio

- **Mapa de nivel de riesgo residual del procedimiento:** en este se anota el código del procedimiento de acuerdo con la calificación obtenida en la tabla resumen del nivel de riesgo residual.

Figura 16
Mapa de riesgo residual del procedimiento.



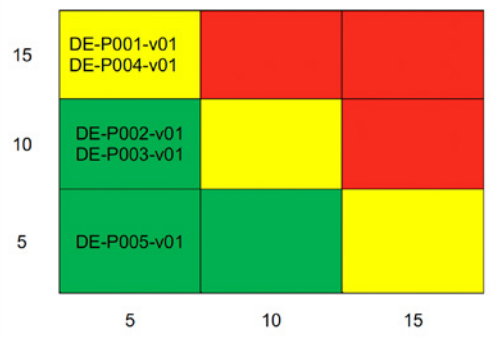
- **Mapa de nivel de riesgos global de la unidad administrativa (pestaña 5):** Esta conformado por la tabla resumen de riesgos de los procedimientos la que se genera automáticamente y propiamente el mapa de nivel de riesgos, donde se coloca en forma manual el número del procedimiento de acuerdo al puntaje obtenido. (Ver tabla 5 y figura 17).

Tabla 5
Resumen nivel de riesgo global de la unidad administrativa

No. Actividad	Código del Procedimiento	Calificación de riesgo residual
1	DE-P001-v01	75
2	DE-P002-v01	70
3	DE-P003-v01	60
4	DE-P004-v01	75
5	DE-P005-v01	25
Nivel de riesgo inherente)		65

Fuente: Elaboración propia Unidad de Control Interno (2022) con base en el Modelo Metodológico SIVAR.

Figura 17
Mapa de nivel de riesgos global de la unidad administrativa.



Plan de acción (pestaña 6)

El Plan de acción constituye un insumo para el informe de seguimiento de las acciones correctivas. Contiene información asociada a las actividades del procedimientos: código del procedimiento, la actividad, tipo de riesgo, factor de riesgo, acción correctiva, estado de la acción, grado de avance, fecha de inicio, fecha de finalización, responsables, actividades y evidencias del cumplimiento. Este plan de acción se genera automáticamente (ver figura 18).

Figura 18
Plan de acción

Plan de acción del SIVAR										
Código del procedimiento.	Nombre del procedimiento	# de Actividad	Presenta Riesgo	Tipo de Riesgo	Factor de riesgo	Indicador	Acción preventiva o correctiva	Estado de la acción	Grado de Avance	Fecha de inicio
SIGLAS-P001-v01	(Nombre del Procedimiento 1)	1	0	0		0	0	0	0%	0/1/1900
SIGLAS-P001-v01	(Nombre del Procedimiento 1)	2	0	0		0	0	0	0%	0/1/1900
SIGLAS-P001-v01	(Nombre del Procedimiento 1)	3	0	0		0	0	0	0%	0/1/1900

Tipos de riesgos (pestaña 7)

Corresponde a la información cuantitativa relacionada con la cantidad de riesgos y los tipos de riesgos a nivel de la unidad administrativa, este se generá automáticamente, y constituye un insumo para el informe de valoración de riesgos anual que brindan las direcciones institucionales.

Figura 19
Tipos de riesgos

TIPO DE RIESGO							
Procedimiento	Objetivo Estratégico n.° 1	Objetivo Estratégico n.° 2	Objetivo Estratégico n.° 3	Legalidad o cumplimiento	Fraude o corrupción	Financiero	Operativo
SIGLAS-P001-v01	0	0	0	0	0	0	0
SIGLAS-P002-v01	0	0	0	0	0	0	0
SIGLAS-P003-v01	0	0	0	0	0	0	0

Otros riesgos

Aquellos riesgos que no se encuentran asociados a las actividades descritas dentro del procedimiento, pero que se identifican como un riesgo potencial, ya sea por una situación interna o externa, y pueden estar asociados a riesgos: operativos, financieros, de cumplimiento, de liderazgo, de cultura organizacional, o ética, fraude o corrupción, tecnología, entre otros; se incluirán al final de los procedimientos de la matriz de riesgos, con la inscripción No aplica "N/A" en el código del procedimiento, número de la actividad y en la actividad propiamente; en el nombre del procedimiento se indicará "otros riesgos" internos o externos, se describe el factor de riesgo y se realiza valoración del riesgo identificado.

18. Anexos

Anexo 1
Portafolio de riesgos de corrupción de la Comisión Nacional de Ética y Valores.[1]

En este portafolio se describen algunos ejemplos de causas o factores de riesgos que corresponden a actos contrarios a la probidad, integridad y ética, que podrían inclusive ser constitutivos de delitos contra los deberes de la función pública, pero no debe entenderse como una lista que abarca todas las opciones posibles:

- Utilizar el cargo oficial con propósitos privados.
- Usar de forma indebida el poder y los recursos públicos para el beneficio personal, el beneficio político particular o el de terceros.
- Participar directa o indirectamente en transacciones financieras, aprovechándose de información confidencial de la cual tengan conocimiento en razón de su cargo, de forma tal que ello les confiera una situación de privilegio de cualquier carácter, para sí, o para terceros, directa o indirectamente.
- Efectuar o patrocinar para terceros, directa o indirectamente, trámites, nombramientos o gestiones administrativas que se encuentren, o no, relacionados con su cargo, salvo lo que está dentro de los cauces normales de la prestación de esos servicios o actividades.
- Usar las instalaciones físicas, el equipo de oficina, vehículos o demás bienes públicos a que tengan acceso, para propósitos ajenos al fin para el que están destinados.
- Aceptar o emitir cartas de recomendación, haciendo uso de su cargo u otros bienes públicos, en beneficio suyo o de un tercero, para procurar nombramientos, ascensos u otros beneficios.
- Desempeñar dos cargos públicos en forma simultánea, salvo casos de excepción expresamente previstos.
- Ofrecer o desempeñar actividades que comprometan su imparcialidad, posibiliten un conflicto de intereses o favorezcan el interés privado en detrimento del interés público.
- Recibir dádivas, obsequios, regalos, premios, recompensas o cualquier otra ventaja como retribución por actos u omisiones inherentes a sus cargos.
- Dar un trato ventajoso a determinadas personas- parientes- en el acceso al empleo público, específicamente aquellos que tienen el poder de nombramiento.
- Dar un uso distinto de los recursos públicos para lo cual fueron asignados.

[1] **Tomado de la Guía para la integración y gestión de riesgos de corrupción en el sistema específico de valoración de riesgos (SEVRI) de la Comisión Nacional de Ética y Valores.**

- No abstenerse, inhibirse o excusarse de realizar un trámite, asunto o procedimiento cuando esté obligado hacerlo.
- Recibir dádivas o cualquier otra ventaja indebida o aceptar la promesa de una retribución de esa naturaleza para hacer un acto propio de sus funciones.
- Recibir dádivas o cualquier otra ventaja o aceptar la promesa directa o indirecta de una retribución de esa naturaleza para hacer un acto contrario a sus deberes o para no hacer o para retardar un acto propio de sus funciones.
- Aceptar dádivas o cualquier otra ventaja indebida por un acto cumplido u omitido en su calidad de funcionario.
- Obligar o inducir a alguien a dar o prometer indebidamente, para sí o para un tercero, un bien o un beneficio patrimonial.
- Influir en un servidor público, prevaliéndose del cargo o de cualquiera otra situación derivada de su situación personal o jerárquica con este o con otro servidor público, ya sea real o simulada, para que haga, retarde u omita un nombramiento, adjudicación, concesión, contrato, acto o resolución propios de sus funciones, de modo que genere, directa o indirectamente, un beneficio económico o ventaja indebidos, para sí o para otro.
- Colocarse en una posición de conflictos de interés.
- Ejecutar maniobras en estados contables con el propósito de generar estados financieros que no reflejan adecuadamente la realidad económica de la institución. (Ejemplos: registro ficticio de ingresos, inadecuado reconocimiento de pérdidas, reporte de activos falsos o sobrevaluados.
- Apropiación o substracción indebida de activos que pueden ser relacionados con efectivo, inventarios y activos fijos, así como robo de información. (Ejemplos: irregularidad anterior a la registración contable, sustracción con posterioridad a la registración, facturas falsas, facturas reales por conceptos falsos o excedidos, robo o alteración de valores, irregularidades a través de esquemas en el proceso de nómina, registros falsos de efectivo para conciliar acciones de fraude, uso indebido del efectivo de la institución y sustracción de activos que no son dinero en efectivo.
- Adulteración o manipulación de documentos o sistemas de información por ejemplo con el fin de obtener beneficio propio o para terceros en labores propias del puesto al modificar, cambiar parcial o completamente documentos o datos, o bien, al impedir, dificultar o condicionar indebidamente el acceso a fuentes de información.
- Fallas en los procesos o problemas estructurales por establecer o mantener trámites de las operaciones complejas poco expeditas, con excesos de requisitos y poco ágiles, que generan retrasos excesivos.
- Falta de transparencia de la información y la gestión por manejar la información pública de manera indebida, ocultar o no disponer de esta para los actores interesados y ciudadanía.
- Aunque no constituyan riesgos de corrupción por sí mismos, desde la ética es importante prestar atención y administrar factores de vulnerabilidad que pueden conducir a la materialización de esos riesgos, por ejemplo:

- Ausencia de canales de comunicación
- Concentración de autoridad o exceso de poder
- Concentración de información de determinadas actividades o procesos en una persona
- Deficiencias en el manejo documental y de archivo
- Deficiente administración del tiempo de trabajo
- Sistemas de información susceptibles de manipulación o adulteración.

Anexo 2
Portafolio de riesgos

	El presente documento incluye una serie de riesgos básicos que pueden presentarse en la implementación y su objetivo es que las Instituciones cuenten con una referencia a la hora de completar la información en las tablas de los procesos. No es una lista exhaustiva de riesgos, cada Institución puede agregar los riesgos que considere necesarios e inclusive puede no aplicar aquellos riesgos que considera no le aplican.
PORTAFOLIO DE RIESGOS	
NORMATIVA TECNOLOGIAS DE LA INFORMACION	
CODIGO	RIESGO EN LA GESTION DE LA INFORMACION
RG01	Abuso de derechos por parte de los usuarios del sistema
RG02	Acceso no autorizado a aplicaciones por parte de los usuarios
RG03	Conformación inadecuada de contraseñas (insegura, débiles)
RG04	Uso compartido de contraseñas por parte de los usuarios
RG05	Robo o perdida de información por controles inadecuados
RG06	Capacitación inadecuada a los usuarios del sistema en la forma de administrar los recursos asignados
RG07	Confidencialidad de la información comprometida
RG07	Privacidad de la información comprometida
RG08	Problemas en el acceso a las aplicaciones
RG09	Integridad de la Información comprometida por usuarios internos
RG10	Integridad de la Información comprometida por accesos externos no autorizados
RG11	No hay disponibilidad de la información
RG12	Clasificación inadecuada de la información
RG13	Etiquetado inadecuado de la in formación
RG14	Robo o perdida de información por ataques de Hackers, Malware
CODIGO	RIESGOS EN LA GESTION DE LA CONTINUIDAD
RC01	Mala identificación de los respaldos de información

	El presente documento incluye una serie de riesgos básicos que pueden presentarse en la implementación y su objetivo es que las Instituciones cuenten con una referencia a la hora de completar la información en las tablas de los procesos. No es una lista exhaustiva de riesgos, cada Institución puede agregar los riesgos que considere necesarios e inclusive puede no aplicar aquellos riesgos que considera no le aplican.

PORTAFOLIO DE RIESGOS	
NORMATIVA TECNOLOGIAS DE LA INFORMACION	
CODIGO	RIESGO EN LA GESTION DE LA INFORMACION
RC02	Respaldos de información no verificados
RC03	Respaldos de información almacenados en forma incorrecta
RC04	Inadecuado traslado y custodia de los respaldos
RC05	Técnicas de recuperación/restauración de los archivos no estandarizada
RC06	Errores en el respaldo y recuperación de los datos.
RC07	Interrupción del servicio por falta de capacidad de almacenamiento o por fallas en los dispositivos de almacenamiento
RC08	Plan de continuidad o contingencia no documentado
RC09	Plan de continuidad o contingencia incompleto
RC10	Plan de continuidad o contingencia no probado
RC11	Plan de continuidad o contingencia no aprobado por las altas autoridades
RC12	Plan de continuidad o contingencia desactualizado
RC13	Personal interno poco preparado para enfrentar una contingencia
RC14	No se cuenta con suficiente personal para enfrentar una contingencia
RC15	Plan de continuidad o contingencia no comunicado a las partes interesadas
RC16	Robo o pérdida de medios de almacenamiento
RC17	Desastres naturales (terremotos, inundaciones, tornados, huracanes, etc.)
RC18	Incendio
RC19	Epidemia

	El presente documento incluye una serie de riesgos básicos que pueden presentarse en la implementación y su objetivo es que las Instituciones cuenten con una referencia a la hora de completar la información en las tablas de los procesos. No es una lista exhaustiva de riesgos, cada Institución puede agregar los riesgos que considere necesarios e inclusive puede no aplicar aquellos riesgos que considera no le aplican.
PORTAFOLIO DE RIESGOS	
NORMATIVA TECNOLOGIAS DE LA INFORMACION	
CODIGO	RIESGO EN LA GESTION DE LA INFORMACION
RC20	Electromagnetismo
RC21	Técnicas de recuperación/restauración de los archivos no estandarizada
RC22	Desorden civil
RC23	Acciones emprendidas por empleados inescrupulosos que pueden causar daños tanto a las instalaciones
RC24	Interrupciones prolongadas de los servicios básicos como la electricidad, el agua potable y las comunicaciones
RC25	Actos criminales, como vandalismo, terrorismo, etc.
RC26	Robo o pérdida de medios de almacenamiento
CODIGO	RIESGOS EN LA GESTION DE LAS COMUNICACIONES
RA01	Fallas en la infraestructura tecnológica de los proveedores externos (ICE. RACSA, CNFL) que soporta la prestación de servicios, afectando la disponibilidad
RA02	Fallas en las comunicaciones debido problemas internos
RA03	Fallas por eventos que afecten las líneas de transmisión internas o externas
RA04	Falta de disponibilidad en las líneas de comunicaciones
RA05	Fallas producidas por errores o problemas en la transmisión
RA06	Errores en la configuración de equipos de comunicaciones
RA07	Monitoreo inadecuado de las comunicaciones
CODIGO	RIESGOS EN CENTROS DE DATOS
RD01	Falta de disponibilidad del personal técnico (SO, base de datos, comunicaciones, etc.)

	El presente documento incluye una serie de riesgos básicos que pueden presentarse en la implementación y su objetivo es que las Instituciones cuenten con una referencia a la hora de completar la información en las tablas de los procesos. No es una lista exhaustiva de riesgos, cada Institución puede agregar los riesgos que considere necesarios e inclusive puede no aplicar aquellos riesgos que considera no le aplican.
PORTAFOLIO DE RIESGOS	
NORMATIVA TECNOLOGIAS DE LA INFORMACION	
CODIGO	RIESGO EN LA GESTION DE LA INFORMACION
RD02	No existe de un plan formal, actualizado y comunicado formalmente para la recuperación de las aplicaciones
RD03	Fallas eléctricas en el centro de cómputo
RD04	Daños que se presenten en los equipos por vandalismo, uso inadecuado o fallas en la administración
RD05	Datos se replican en forma incorrecta
RD06	Fallas en el equipo de aire acondicionado, UPS o planta eléctrica
RD07	Controles inadecuados para el monitoreo, seguimiento y protocolos formales para atención y escalamiento de incidentes
RD08	Aplicaciones anticuadas que no soportan la carga de trabajo, el volumen, las funcionalidades
RD09	Inadecuado mantenimiento de los sistemas
RD10	Reprocesos en las pruebas y atrasos en la implementación por no contar con una infraestructura para la realización de las pruebas técnicas
RD11	Dependencia de los proveedores para el suministro de servicios, repuestos o de mantenimientos a los equipos donde corren los sistemas críticos
RD12	Utilización incorrecta de los equipos de cómputo
RD13	Mal funcionamiento de una base de datos
RD14	Daño en una base de datos o archivos críticos
RD15	Problemas de acceso a una base de datos
RD16	Administración inadecuada de procesos de actualización

	El presente documento incluye una serie de riesgos básicos que pueden presentarse en la implementación y su objetivo es que las Instituciones cuenten con una referencia a la hora de completar la información en las tablas de los procesos. No es una lista exhaustiva de riesgos, cada Institución puede agregar los riesgos que considere necesarios e inclusive puede no aplicar aquellos riesgos que considera no le aplican.
PORTAFOLIO DE RIESGOS	
NORMATIVA TECNOLOGIAS DE LA INFORMACION	
CODIGO	RIESGO EN LA GESTION DE LA INFORMACION
RD17	Falta de capacitación o capacitación inadecuada de los encargados de los procesos de actualización
RD18	Falta de procedimientos o procedimientos inadecuados para la ejecución de tareas críticas
RD19	Controles deficientes en ambientes de pruebas
RD20	Controles deficientes en ambientes de producción
RD21	Falla en un servidor o varios a la vez
RD22	Pérdidas o suspensión temporal del servicio por una incorrecta configuración de parámetros en los sistemas
RD23	Errores en la configuración de equipos (servidores)
RD24	Mal diseño de las aplicaciones generando problemas de funcionamiento
RD25	Problemas en la distribución del cableado eléctrico o de comunicaciones
RD26	Insuficiente personal capacitado para realizar las tareas de operación, monitoreo y soporte de los servicios en producción
RD27	Afectación en la gestión y los programas de trabajo porque no se realizaron las pruebas de aceptación dentro del tiempo planificado
RD28	Inundación por daño de tuberías internas del edificio
RD29	Fallas producidas por errores de programación que afectan la calidad del servicio
RD30	Afectación del servicio por generación de incidentes y problemas asociados a una mala implementación de cambios
RD31	Afectación del servicio por no tramitar oportunamente un cambio requerido urgente

	El presente documento incluye una serie de riesgos básicos que pueden presentarse en la implementación y su objetivo es que las Instituciones cuenten con una referencia a la hora de completar la información en las tablas de los procesos. No es una lista exhaustiva de riesgos, cada Institución puede agregar los riesgos que considere necesarios e inclusive puede no aplicar aquellos riesgos que considera no le aplican.
PORTAFOLIO DE RIESGOS	
NORMATIVA TECNOLOGIAS DE LA INFORMACION	
CODIGO	RIESGO EN LA GESTION DE LA INFORMACION
RD32	Reprocesos en las pruebas y atrasos en la implementación por integración de aplicaciones incompletas o erróneas
RD33	Pérdida de información producidas por fallas en los controles de seguridad
RD34	Pérdida de información por la inadecuada utilización de los equipos de cómputo
RD35	No contar con las condiciones ambientales recomendadas por el fabricante para la operación adecuada de los equipos
RD36	Pérdida de información por la inadecuada utilización de los sistemas en utilización en la Institución
CODIGO	RIESGOS EN LA GESTION DE PROVEEDORES
RP01	Incumplimiento de contratos por parte del proveedor
RP02	Incumplimiento de contratos por parte de la Institución
RP03	Deficiencias en los servicios de los proveedores
RP04	No contar con proveedores que estén preparados para ayudar a enfrentar una contingencia de tipo tecnológico.
RP05	Alta dependencia de proveedores claves a nivel de tecnología para proporcionar los servicios
RP06	Contratos obsoletos
RP07	Fallas en la gestión de licenciamientos
RP08	Fallas en el control de vencimiento de los contratos
RP09	Inexistencia de contratos
RP10	Contratos no alineados a niveles de servicio (SLA)

	El presente documento incluye una serie de riesgos básicos que pueden presentarse en la implementación y su objetivo es que las Instituciones cuenten con una referencia a la hora de completar la información en las tablas de los procesos. No es una lista exhaustiva de riesgos, cada Institución puede agregar los riesgos que considere necesarios e inclusive puede no aplicar aquellos riesgos que considera no le aplican.
PORTAFOLIO DE RIESGOS	
NORMATIVA TECNOLOGIAS DE LA INFORMACION	
CODIGO	RIESGO EN LA GESTION DE LA INFORMACION
CODIGO	RIESGOS DE CUMPLIMIENTO
RI01	Incumplimiento por entrega de información incompleta a entes reguladores
RI02	Incumplimiento de la legislación vigente
RI03	Incumplimiento de normativas externas
RI04	Incumplimiento en las fechas de entrega de la información a entes reguladores
RI05	No contar con el apoyo de las altas autoridades
RI06	Insuficientes recursos (humanos, equipos, espacio físico, etc.) para trabajar en la implementación
RI07	No contar con una cultura de riesgos en la institución
RI08	Los responsables de TI no cuentan con el suficiente apoyo de las altas autoridades para realizar su gestión
RI09	No se cuenta con políticas institucionales para la gestión de TI
CODIGO	RIESGOS EN SEGURIDAD DE LA INFORMACION
RS01	Incumplimiento de políticas de seguridad
RS02	Falta de capacitación y concientización en seguridad de la información
RS03	Políticas de seguridad no documentadas o están desactualizadas
RS04	Normativas de seguridad no documentadas o están desactualizadas
RS05	Controles de seguridad no documentadas o están desactualizadas
RS05	Procedimientos de seguridad no documentadas o están desactualizadas
RS07	Procesos de seguridad no documentados o están desactualizadas

MINISTERIO DE CIENCIA, INNOVACIÓN, TECNOLOGÍA Y TELECOMUNICACIONES	El presente documento incluye una serie de riesgos básicos que pueden presentarse en la implementación y su objetivo es que las Instituciones cuenten con una referencia a la hora de completar la información en las tablas de los procesos. No es una lista exhaustiva de riesgos, cada Institución puede agregar los riesgos que considere necesarios e inclusive puede no aplicar aquellos riesgos que considera no le aplican.
PORTAFOLIO DE RIESGOS	
NORMATIVA TECNOLOGIAS DE LA INFORMACION	
CODIGO	RIESGO EN LA GESTION DE LA INFORMACION
RS08	Ataques de denegación de servicios
RS09	No se actualiza en forma adecuada la plataforma tecnológica que atiende los servicios de Internet
RS10	Plataforma de seguridad mal atendida, monitoreo inadecuado de incidentes de seguridad
RS11	Capacitación inadecuada en ingeniería social
RS12	Perdida de equipos de cómputo (principalmente portátiles) sin la debida protección, con la consiguiente pérdida de información confidencial).
RS13	Perfiles de acceso no definidos o mal configurados.
RS14	Red interna puede ser vulnerada por parte de cibercriminales
RS15	Gestión inadecuada en el parchado de aplicaciones o equipos

Referencias Bibliográficas:

Comisión Nacional de Ética y Valores.(2020) *Guía para la integración y gestión de riesgos de corrupción en el sistema específico de Valoración de riesgos (SEVRI).*

Contraloría General de la República. *Curso Virtual "Control Interno" Componente 2 Valoración del Riesgo.* (2011)

Guía técnica para el desarrollo de auditorías de la ética, (GT-01-2008). Contraloría General de la República

Ley General de Control Interno n.°8292 del 31 de julio de 2002.

Normas de control interno para el Sector Público (N-2-2009-CO-DFOE) Publicado en La Gaceta N.°26 del 6 de febrero de 2009.

Tribunal Supremo de Elecciones. *Plan estratégico institucional PEI 2019-2024*

Tribunal Supremo de Elecciones. *Guía para completar la matriz de riesgos del SIVAR* (2017)

MISIÓN

Impartir justicia electoral, organizar y arbitrar procesos electorales transparentes y confiables, capaces por ello de sustentar la convivencia democrática, así como prestar los servicios de registración civil e identificación de los costarricenses.

VISIÓN

Ser un organismo electoral líder de Latinoamérica, tanto por su solvencia técnica como por su capacidad de promover cultura democrática.

Dirección EJECUTIVA
TRIBUNAL SUPREMO DE ELECCIONES

Unidad de Control Interno

Costado Oeste del Parque Nacional, Calle 15, Avenidas 1 y 3.
Central Telefónica: 2287-5555. Apartado: 2163-1000, San José.
www.tse.go.cr