

Ministerio de la Presidencia de la República  
Instituto Costarricense sobre Drogas  
Unidad “Planificación Institucional”

Guía metodológica para  
el fortalecimiento y el perfeccionamiento del  
Sistema de Control Interno Institucional

---



2022

## Contenido

Presentación.....	4
Componentes del SCI- Marco Orientador .....	5
1. Normativa jurídica.....	5
Normativa de la Contraloría General de la República.....	5
2. Normativa técnica .....	5
3. Marco estratégico-operativo .....	6
Política para la gestión del riesgo institucional.....	6
Objetivos de la gestión del riesgo institucional .....	6
4. Control interno.....	6
Definición .....	6
Compromiso institucional para el adecuado funcionamiento del SCI.....	6
5. Sistema Específico de Valoración de Riesgos Institucionales (SEVRI).....	7
6. Ambiente de Control.....	8
Administración activa-sujetos interesados .....	8
Recursos disponibles .....	9
Herramientas de apoyo a la información.....	10
Definición e importancia del SEVRI .....	10
7. Estrategia para el fortalecimiento y el perfeccionamiento del SEVRI.....	11
Etapa 1: Identificación de riesgos .....	11
Etapa 2: Análisis de riesgos .....	13
Etapa 3: Valoración (evaluación) de riesgos .....	14
Etapa 4: Administración de los riesgos .....	17
Etapa 5: Revisión de riesgos.....	20
Etapa 6: Documentación de riesgos.....	20
Etapa 7: Comunicación de riesgos .....	21
8. Glosario .....	22
9. Fuentes consultadas y de referencia.....	24
10. Anexos.....	26

## Índice de tablas

Tabla 1. Criterios para establecer la probabilidad o frecuencia del riesgo.....	14
Tabla 2. Criterios para establecer el impacto o la consecuencia del riesgo .....	14
Tabla 3. Nivel de exposición al riesgo según impacto y probabilidad.....	15
Tabla 4. Criterios de aceptación del riesgo, según nivel de riesgo y tipo de administración. ....	16

## Índice de figuras

Figura 1. Estructura del SEVRI-ICD, a nivel de POSI .....	7
Figura 2. Administración activa-sujetos interesados .....	9

## Anexos

Anexo 1. Técnicas para la identificación y el análisis del riesgo institucional.....	26
Anexo 2. Listado de categorías de riesgos institucionales del ICD.....	27
Anexo 3. Matriz para la identificación del riesgo institucional, según procesos y objetivos de la POSI .....	37
Anexo 4. Matriz para la valoración del riesgo institucional, según procesos y objetivos de la POSI	37
Anexo 5. Matriz para la valoración de la madurez de las medidas administrativas existentes.....	38
Anexo 6. Matriz para la priorización de los riesgos institucionales a administrar.....	39
Anexo 7. Programación de la actividad de respuesta al riesgo seleccionada para su ejecución.....	42

## Ficha de control de cambios

Fecha	N° de versión	Elaborado por:
2018	V1.	UPLA
2019	V2.	UPLA
2022	V3.	UPLA

## Presentación

Se espera que esta guía se constituya en el principal insumo para que las personas funcionarias del Instituto Costarricense sobre Drogas (ICD) puedan:

- Reconocer la importancia del Control Interno (CI) y la legislación que lo sustenta, así como su estructura y demás componentes funcionales/orgánicos.
- Concebir al Sistema Específico de Valoración de Riesgos Institucionales (SEVRI) como un componente del control interno y su relación con los objetivos institucionales.
- Tener claro qué es un riesgo y cómo éste se puede reconocer a nivel institucional.
- Identificar cada una de las etapas del SEVRI y cómo ponerlas en práctica con respecto a los objetivos que las Unidades y Órganos staff definan en la Programación Operativa Sustantiva Institucional (POSI).

En el apartado denominado *“Anexos”*, encontrará un conjunto de plantillas que servirán como ejemplo para guiar el análisis en la identificación y la valoración de los riesgos, así como, el ordenamiento, el registro y la documentación de estos esfuerzos. Además, en la carpeta compartida *“Público”*, específicamente en *“UNIDAD “PLANIFICACIÓN INSTITUCIONAL”\CONTROL INTERNO Y SEVRI\Plantillas SEVRI”*, dispondrá de dichas plantillas.

Complementariamente, los funcionarios enlace de la UPLA contarán con el documento *“Guía para la actualización del SEVRI en el SIGMA”* que explica cómo realizar el registro, el monitoreo y la evaluación del sistema desde el *“Sistema de Gestión y Monitoreo de Actividades”* (SIGMA), en la plataforma *“ICD Portal”*.

## Componentes del SCI- Marco Orientador

### 1. Normativa jurídica

#### Normativa de la Contraloría General de la República

La normativa que da fundamento al Sistema de Control Interno costarricense y, por ende, base para el desarrollo del presente apoyo documental, parte de lo estipulado en la Ley N° 8131, "*Ley de la Administración Financiera y Presupuestos Públicos*" (artículos 17 y 18), y en la Ley N° 7428, "*Ley Orgánica de la Contraloría General de la República*" (artículos 24 y 60), que le otorga facultades a la Contraloría General de la República (CGR) en materia de control interno. En cumplimiento de este mandato, la CGR pone a disposición para acatamiento obligatorio, entre otros instrumentos jurídicos<sup>1</sup>, cuatro cuerpos normativos, a saber:

- Ley N°8292, "*Ley General de Control Interno*" de 2002.
- N-2-2009-CO-DFOE, "*Normas de control interno para el Sector Público*" de 2009.
- D-3-2005-CO-DFOE, "*Directrices Generales para el establecimiento y funcionamiento del Sistema de Valoración del Riesgo*" de 2005.
- N-2-2007-CO-DFOE, "*Normas Técnicas para la gestión y el control de las Tecnologías de Información*" de 2007.

### 2. Normativa técnica

Con el objetivo de guiar a las personas funcionarias del ICD en el acatamiento de la norma jurídica antes señalada se crearon dos instrumentos, a saber:

- Guía metodológica para el fortalecimiento y el perfeccionamiento del Sistema de Control Interno Institucional; y
- El Catálogo de Riesgos Institucional.

Se aclara que los instrumentos señalados se encuentran alineados a la plataforma jurídica que desde la CGR se ha emitido en materia de control interno.

---

<sup>1</sup> La normativa completa se encuentra disponible para su consulta en: <https://www.cgr.go.cr/03-documentos/normativa/control-interno.html>

### 3. Marco estratégico-operativo

El ICD aprobó a través del Plan Estratégico Institucional (PEI) 2022-2026, la Política para la Gestión del Riesgo Institucional, la cual es de acatamiento obligatorio. Seguidamente el detalle de dicho enunciado:

#### Política para la gestión del riesgo institucional

*“Fortalecimiento del control interno mediante el diseño y puesta en operación de acciones dirigidas a aportar seguridad razonable en la consecución de los objetivos definidos en las leyes N°8204 y N°8292” (ICD, 2022).*

#### Objetivos de la gestión del riesgo institucional

- *“Sensibilizar a las personas funcionarias del ICD en temas relacionados a esta materia, para la protección y conservación del patrimonio público contra cualquier pérdida, despilfarro, uso indebido, irregularidad o demás actos ilegales.*
- *Crear los controles necesarios a favor de la eficiencia y la eficacia de las operaciones institucionales, así como de la integridad, la transparencia, la confiabilidad y la oportunidad de la información generada” (ICD, 2022).*

### 4. Control interno

La Ley N°8292 establece para cada institución pública, la obligatoriedad de disponer de un Sistema de Control Interno (SCI), así como, de mantenerlo, perfeccionarlo y evaluarlo.

#### Definición

El control interno es el conjunto de acciones diseñadas y ejecutadas para aportar seguridad (razonable) en el logro de los objetivos institucionales (Ley N°8292).

Objetivos del CI según la Ley N°8292

1. *“Proteger y conservar el patrimonio público contra cualquier pérdida, despilfarro, uso indebido, irregularidad o acto ilegal.*
2. *Exigir confiabilidad y oportunidad de la información.*
3. *Garantizar eficiencia y eficacia de las operaciones.*
4. *Cumplir con el ordenamiento jurídico y técnico” (Ley N°8292, Art.8).*

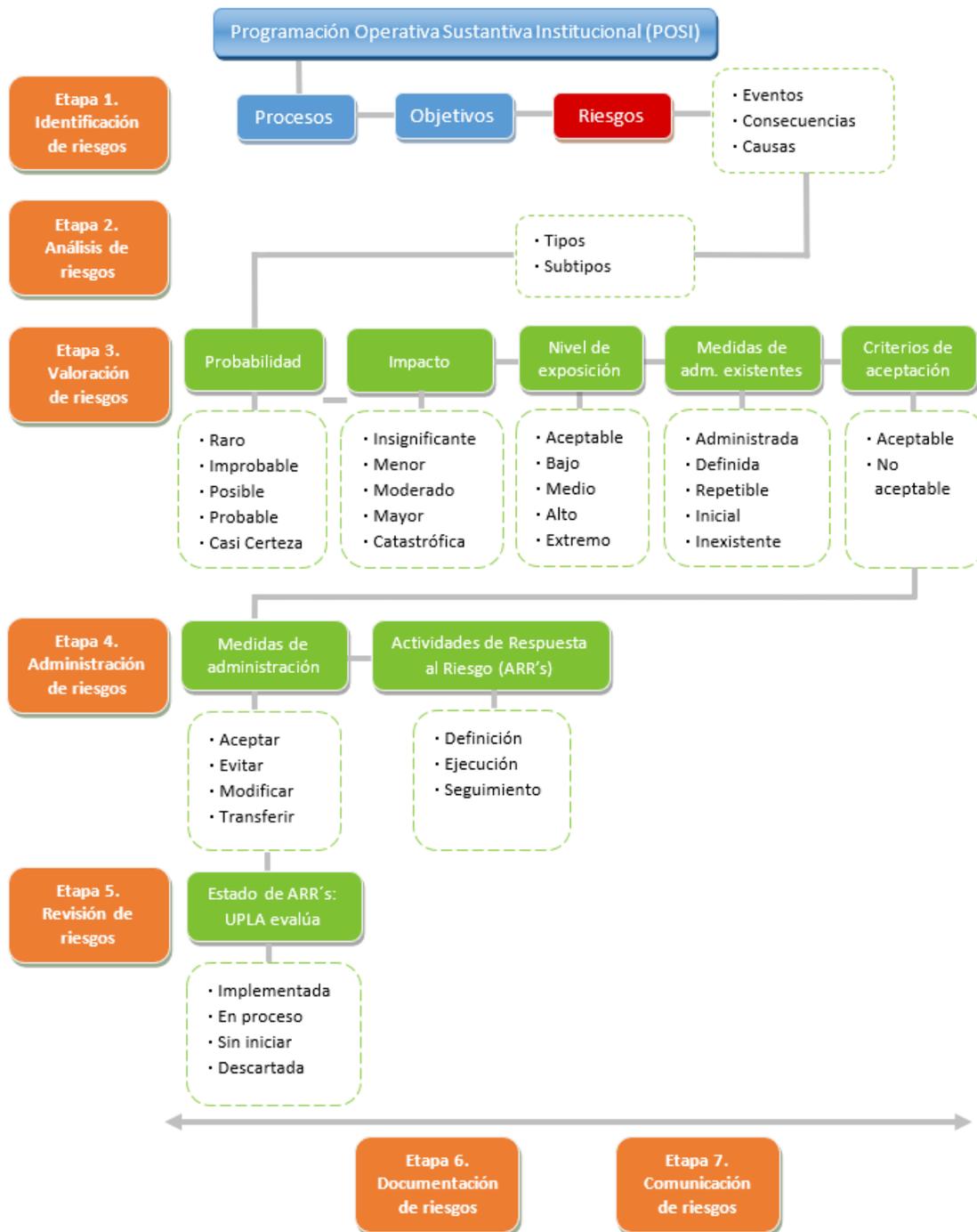
#### Compromiso institucional para el adecuado funcionamiento del SCI

De conformidad con las responsabilidades que competen a cada puesto de trabajo, el jerarca y los funcionarios deben, de manera **oportuna, efectiva y atendiendo** la normativa, efectuar las **acciones** necesarias y acoger los **requerimientos** (solicitudes) para el debido **diseño, operación, y fortalecimiento de los componentes del CI** (CGR, 2009). Asimismo, el compromiso institucional liderado por los jefes y el personal se encausa en el cumplimiento de la política de gestión del riesgo institucional y sus objetivos enunciados anteriormente.

## 5. Sistema Específico de Valoración de Riesgos Institucionales (SEVRI)

La valoración del riesgo institucional es un componente del CI, y para su tratamiento, cuenta con la herramienta SEVRI, gestionada mediante la plataforma SIGMA. Lo expresado, se puede observar en el *Diagrama 1*. Se recuerda que, el documento “*Guía para la actualización del SEVRI en el SIGMA*” detalla como registrar, monitorear y evaluar el SEVRI desde el SIGMA.

Figura 1. Estructura del SEVRI-ICD, a nivel de POSI



Fuente: Elaboración propia, UPLA, 2018.

## 6. Ambiente de Control

### Administración activa-sujetos interesados

---

En acatamiento a la Ley General de Control Interno, artículos 9, 10 y 11, que rezan:

*“Artículo 9º.-Órganos del sistema de control interno. La administración activa y la auditoría interna de los entes y órganos sujetos a esta Ley serán los componentes orgánicos del sistema de control interno establecido e integrarán el Sistema de Fiscalización Superior de la Hacienda Pública a que se refiere la Ley Orgánica de la Contraloría General de la República.*

*Artículo 10.-Responsabilidad por el sistema de control interno. Serán responsabilidad del jerarca y del titular subordinado establecer, mantener, perfeccionar y evaluar el sistema de control interno institucional. Asimismo, será responsabilidad de la administración activa realizar las acciones necesarias para garantizar su efectivo funcionamiento.*

*Artículo 11.-El sistema de control interno en la desconcentración de competencias y la contratación de servicios de apoyo. El jerarca y los titulares subordinados tendrán la responsabilidad de analizar las implicaciones en el sistema de control interno, cuando se lleve a cabo una desconcentración de competencias, o bien la contratación de servicios de apoyo con terceros; asimismo, la responsabilidad de tomar las medidas correspondientes para que los controles sean extendidos, modificados y cambiados, cuando resulte necesario”.*

... el Instituto Costarricense sobre Drogas define como sujetos interesados y Administración Activa a las personas funcionarias de la entidad que ocupan cargos políticos, técnicos y operativos, formalizados tanto en la estructura ocupacional como en la estructura organizativa institucional<sup>2</sup>.

Si bien es cierto, las labores de seguimiento y de evaluación son responsabilidad directa de los actores decisores, sean políticos o técnicos, también es cierto que la responsabilidad de fortalecer y perfeccionar el SEVRI y el SCI recae en el cien por ciento de las personas funcionarias del ICD.

---

<sup>2</sup> Para ampliar información respecto a la cantidad de actores involucrados se invita atentamente a consultar el PEI 2022-2026: “Figura 7. Organigrama por perfil ocupacional, 2021”, página 26.

Para ilustrar lo señalado, observar el siguiente diagrama:

Figura 2. Administración activa-sujetos interesados



Fuente: Elaboración propia, UPLA, 2022.

### Recursos disponibles

Recursos disponibles para la implementación y mejora del SCI-ICD

Recurso	Detalle
Humano	<ul style="list-style-type: none"> <li>• Jerarcas institucionales.</li> <li>• Titulares subordinados.</li> <li>• La Auditoría Interna (AI) dispone de una Auditora como jefa y tres personas funcionarias a su cargo.</li> <li>• La Unidad “Planificación Institucional” (UPLA) cuenta con una jefatura y una profesional que desarrollan acciones para el fortalecimiento y monitoreo del SCI-ICD.</li> </ul> <p>Periódicamente, tanto la AI como la UPLA brindan a las personas funcionarias del ICD capacitación, formación, asesoría y acompañamiento para el desarrollo de actividades relacionadas con el tema.</p>
Financiero	Se cuenta únicamente con el presupuesto ordinario asignado al ICD, con todas las limitaciones que, las actuales políticas de Estado, emitidas desde el Ministerio de Hacienda generan.
Técnico	<p>Refiere a todos los instrumentos creados y avalados por los jefarcas del ICD, como por ejemplo:</p> <ul style="list-style-type: none"> <li>• Procedimientos.</li> <li>• Manuales.</li> <li>• Guías.</li> <li>• Directrices.</li> <li>• Controles, como bitácoras, contraseñas, autorizaciones, etc.</li> </ul>

<i>Recurso</i>	<i>Detalle</i>
Tecnológico	<ul style="list-style-type: none"> <li>• Entre otros.</li> </ul> <p>El módulo “Sistema de Gestión y Monitoreo de Actividades” (SIGMA) dentro de ICD Portal, es el sistema informático en el que se lleva el registro y el monitoreo de diferentes instrumentos de gestión institucional. A nivel de la planificación operativa institucional se desarrolla todo el apartado correspondiente al SEVRI.</p> <p>Asimismo, los sistemas informáticos con los que cuentan las instancias organizacionales, los cuales disponen de medidas para el aseguramiento de la información.</p> <p style="text-align: right;"><b>Fuente:</b> Elaboración propia, 2022.</p>

### Herramientas de apoyo a la información

Como herramienta tecnológica y de apoyo para la administración de la información, el ICD dispone del SIGMA, instrumento detallado en el componente “Tecnológico”, apartado “*Recursos Disponibles*”.

Si bien han existido otras versiones del SIGMA, el modelo actual data desde 2012, y corresponde a la segunda versión.

Todas las personas funcionarias tienen compromisos bajo su responsabilidad en materia de riesgos, pero solo algunos tienen autorizado por sus respectivas jefaturas para acceder al SIGMA sea para: ingresar nuevos riesgos, actualizar existentes o sus niveles de exposición, registrar nuevas ARR, rendir cuentas o descargar mapas de riesgo, reportes históricos de los riesgos institucionales, de las causas y consecuencias, el nivel de exposición y las medidas de administración del riesgo.

Dentro del SIGMA, se encuentra disponible un apartado de ayuda al usuario, el cual se complementa con el documento “*Guía para la actualización del SEVRI en el SIGMA*” elaborado por la UPLA.

### Definición e importancia del SEVRI

Es el conjunto organizado de componentes para la identificación, el análisis, la evaluación, la administración, la revisión, la documentación y la comunicación de los riesgos institucionales relevantes (CGR, 2005). Con el SEVRI se obtiene:

- Información actualizada sobre riesgos institucionales.
- Medidas para la administración de riesgos.
- Niveles de riesgo aceptables.
- El logro de los objetivos institucionales.

## 7. Estrategia para el fortalecimiento y el perfeccionamiento del SEVRI

Con el objetivo de avanzar a niveles de madurez superiores, seguidamente y por etapas, se presentan aquellos componentes funcionales que conforman el citado sistema.

### Etapa 1: Identificación de riesgos

La identificación de riesgos es clave, pues al partir del reconocimiento de cuáles son los procesos, objetivos y actividades que realiza cada Unidad para el cumplimiento de sus funciones, permite alcanzar una mejor comprensión sobre cómo las labores diarias y estratégicas se encuentran expuestas a la incertidumbre y por ende, al riesgo.

**¿Qué se comprende por riesgo?**: El diccionario Oxford conceptúa el término riesgo como la *“posibilidad de que se produzca un contratiempo o una desgracia, de que alguien o algo sufra perjuicio o daño”* (Oxford, s.a.). En una organización, es aquel evento o situación interna o externa que podría producirse en algún momento dado y tener consecuencias sobre el objetivo que persigue una Unidad. En otras palabras, es *“la posibilidad de que suceda algo que tendría un impacto sobre los objetivos institucionales”* (CGR, 2011, p.2), ya sea que estos refieran al Plan Nacional Sobre Drogas, Legitimación de Capitales y Financiamiento al Terrorismo (PNsD) o a la Programación Operativa Sustantiva Institucional (POSI) vigente.

Cada Unidad (o inter-Unidad), a través de los instrumentos de gestión (PNsD y POSI), define sus compromisos por proyectos (PNsD) y por procesos (POSI), y dentro de estos, sus objetivos. En el caso de la POSI, es sobre los objetivos que se realizará la identificación y administración de los riesgos potenciales (reiterando que, los riesgos son aquellas amenazas que puedan afectar el desarrollo de las actividades dirigidas al logro de estos).

### ¿Cómo reconocer un riesgo institucional?

#### PASO 1. Identificando eventos existentes y posibles:

Es conveniente, en cada proceso, objetivo, etapa y actividad, conjuntamente como Unidad o inter-Unidad preguntarse: *“¿qué puede suceder?”*, seguidamente, se enlistan aquellos elementos, condiciones o situaciones que afecten o puedan causar afectación sobre los procesos de la (s) Unidad (es) y, por ende, a los objetivos que persiguen.

### ¿Qué es un riesgo institucional y qué no lo es?

- **Un riesgo laboral NO es un riesgo institucional:** (NO constituyen riesgos institucionales: riesgos higiénicos, exposición a sustancias tóxicas, poca iluminación, exceso de ruido, riesgos ergonómicos -optimización del espacio y condiciones de trabajo-, carga física, mental, social, etc.). A menos que revelen fallas y debilidades estructurales recurrentes, y no, casos aislados. Para efectos de la identificación de riesgos que atenten contra la consecución de los objetivos institucionales, no se considerarán los riesgos laborales; estos corresponden a materia de salud ocupacional.

- **Un riesgo personal NO es un riesgo institucional:** puesto que se entiende por riesgos personales los “*que producen daños en la integridad de las personas y que provocan pérdidas económicas importantes para ellos o sus familias*”<sup>3</sup> (Equivida, Riesgos personales, s.a.) Por ejemplo: el riesgo sobre la vida y la salud de un funcionario que no practica hábitos alimenticios y deportivos saludables, no se reconoce como un riesgo institucional.
- **Un riesgo ambiental NO es un riesgo institucional:** desastres naturales o provocados por el ser humano (inundaciones, incendios), si bien, atentan contra la normal labor diaria de la población bajo sus efectos, no son asociados directamente, como producto de los procesos y tareas con las que, las Unidades alcanzan sus objetivos propuestos.

## PASO 2. Reconociendo sus causas y consecuencias:

**Causa:** Se refiere al origen del riesgo (interno o externo). Al identificar la causa, se facilita la comprensión y clasificación del riesgo (en categorías). Es importante reconocer la causa primaria, es decir, aquella que origina el riesgo.

**Consecuencias/impactos:** son los efectos o resultados producidos al ocurrir el riesgo.

### EJEMPLO:

**Causa:** No existe una división de funciones y niveles de autorización. Ejemplo: En la empresa “ABC” un funcionario del departamento de adquisiciones (Proveeduría) concentra las facultades para solicitar, tramitar y autorizar la compra de materiales.

**Riesgo potencial:** Corrupción. Existe la posibilidad de que compre materiales de oficina innecesarios y los sustraiga, para posteriormente obtener un beneficio personal.

**Impacto:** a nivel de recursos. Significa una pérdida económica para la institución. (Auditoría Superior de la Federación -ASF-, s.a.).

Realizar los ejercicios 1 y 2. Posteriormente, consultar la solución de los mismos. Estos los encontrará en la carpeta “SEVRI” de la Unidad “Planificación Institucional”, ubicada en la carpeta “Público”.

La identificación del riesgo debe realizarse de manera conjunta entre todos los funcionarios que integran una Unidad, considerando los procesos y los objetivos que se tienen para el periodo en análisis. Para eso, se sugiere acceder al **Anexo 1. Técnicas para la identificación y el análisis del riesgo institucional**, se enlistan una serie de técnicas que pueden facilitar el ejercicio de identificación y análisis de riesgos. Para organizar y documentar este ejercicio, se recomienda el empleo de una tabla sencilla que enliste el proceso, el objetivo, el riesgo, su descripción, sus causas o la causa primaria, y sus consecuencias, como la que aparece en el **Anexo 3. Matriz para la identificación del riesgo institucional, según procesos y objetivos de la POSI**.

<sup>3</sup> Tomado de: <https://www.equivida.com/tipos-de-riesgo>.

Una vez realizado el ejercicio de enlistar los riesgos posibles, sus causas y consecuencias, los mismos se clasifican en tipos.

### **Clasificación de los riesgos por categorías:**

Esta clasificación responde a categorías contenidas dentro del SIGMA, ya definidas por la Unidad “Planificación Institucional” (UPLA), y que se pueden consultar en el *Anexo 2. Listado de categorías de riesgos institucionales del ICD*”.

Este ejercicio se puede registrar en la misma tabla del *Anexo 3. Matriz para la identificación del riesgo institucional, según procesos y objetivos de la POSI*. Recalcando, esta matriz puede considerarse un paso previo para organizar el análisis, identificar los riesgos más relevantes y críticos, y facilitar el ingreso de esta información en el SIGMA.

Es necesario señalar, que no todos los riesgos se pueden atender, pues su administración puede implicar costos económicos e inversión de tiempo, por lo que, Si el ejercicio genera una amplia cantidad de riesgos por cada objetivo de cada proceso, se priorizan aquellos, que consensuadamente, se reconozcan como los más relevantes. Nuevamente la matriz del anexo 4, puede ayudar en esta priorización.

### Etapa 3: Valoración (evaluación) de riesgos

En esta etapa, cada riesgo recibe una calificación sobre una serie de criterios. La finalidad es reconocer el grado de amenaza que representa cada riesgo identificado y qué tan susceptible es el ICD ante estos. La valoración también debe ser un ejercicio conjunto y consensuado, entre el personal de la (s) Unidad (es).

#### *PASO 1. Determinación de la probabilidad*

**Probabilidad (frecuencia):** Se le asigna un valor o peso a la frecuencia con la que el riesgo podría ocurrir.

**Tabla 1.** Criterios para establecer la probabilidad o frecuencia del riesgo

Probabilidad	Criterios
Excepcional	Se considera que el evento tiene una posibilidad mínima de suceder. Podría ocurrir en un lapso <b>mayor a 5 años</b> .
Esporádica	Se considera que el evento tiene una posibilidad leve de suceder. Podría ocurrir al menos <b>una vez cada 5 años</b> .
Moderada	Se considera que el evento tiene una posibilidad moderada de suceder. Podría ocurrir <b>una vez cada año</b> .
Frecuente	Se considera que el evento tiene una posibilidad alta de suceder. Podría ocurrir en forma periódica, <b>una vez por semestre</b> .
Siempre	Se considera que la posibilidad de ocurrencia del evento es permanente. Podría ocurrir <b>cuando menos una vez por mes</b> .

**Fuente:** Elaboración propia de la UPLA 2018, con base en Universidad Nacional (UNA), 2018.

#### *PASO 2. Determinación del impacto (consecuencias)*

Se trata de estimar el grado de afectación negativa (probable) sobre el logro de los objetivos de la Unidad, que se pueda generar como consecuencia del riesgo no atendido.

**Tabla 2.** Criterios para establecer el impacto o la consecuencia del riesgo

Impacto	Criterios
Mínimo	Se estima que el logro del objetivo se afectaría en <b>menos de un 10%</b> .
Menor	Se estima que el logro del objetivo se afectaría entre un <b>10%</b> y menos de un <b>20%</b> .
Significativo	Se estima que el logro del objetivo se afectaría entre un <b>20%</b> y menos de un <b>30%</b> .
Mayor	Se estima que el logro del objetivo se afectaría entre un <b>30%</b> y menos de un <b>50%</b> .
Muy severo	Se estima que el logro del objetivo se afectaría en <b>50% o más</b> .

**Fuente:** Elaboración propia de la UPLA 2018, con base en SIGMA y UNA, 2018.

En el SIGMA, se incorpora el espacio “Justificación” para argumentar la valoración que se hizo del riesgo según su probabilidad de ocurrencia y el posible impacto que tenga sobre los objetivos de la Unidad, en caso de materializarse.

*PASO 3. Nivel de exposición al riesgo*

Al seleccionar el grado de probabilidad y de impacto estimados, automáticamente la tabla del **Anexo 4. Matriz para la valoración del riesgo institucional, según procesos y objetivos de la POSI**, así como el SIGMA, calculan el nivel de exposición al riesgo. Únicamente para efectos de su comprensión, se presenta la tabla 3 con los porcentajes de exposición:

**Tabla 3.** Nivel de exposición al riesgo según impacto y probabilidad.

<b>Impacto Probabilid.</b>	<b>Mínimo</b>	<b>Menor</b>	<b>Significativo</b>	<b>Mayor</b>	<b>Severo</b>
Excepcional	Aceptable 4%	Aceptable 8%	Aceptable 12%	Bajo 16%	Bajo 20%
Esporádico	Aceptable 8%	Bajo 16%	Bajo 24%	Medio 32%	Medio 40%
Moderado	Aceptable 12%	Bajo 24%	Medio 36%	Alto 48%	Alto 60%
Frecuente	Bajo 16%	Medio 32%	Alto 48%	Extremo 64%	Extremo 80%
Casi siempre	Bajo 20%	Medio 40%	Alto 60%	Extremo 80%	Extremo 100%

**Fuente:** Elaboración propia con base en el programa SIGMA.

PASO 4. Criterios de aceptación del riesgo

Los niveles de exposición indicados en la tabla anterior responden a la normativa vigente, en la cual, el ICD se basa para determinar los criterios de aceptación del riesgo, comprendidos como los niveles que la institución identifica como aceptables o no, y según esto, define cómo se va a administrar el mismo.

**Tabla 4.** Criterios de aceptación del riesgo, según nivel de riesgo y tipo de administración.

Nivel de exposición al riesgo	Criterio de aceptación	Administración del riesgo
Aceptable 	<b>Aceptable:</b> Riesgo menor o igual que 15%.	Se da por concluido el proceso de gestión de riesgos. Es decir, hasta aquí se llega con el tratamiento del riesgo, pues no requiere tomar medidas para su atención, más, que realizar un monitoreo periódico (repetir los pasos anteriores) a fin de determinar si sale o no del rango aceptable. En caso de que, en un próximo monitoreo, supere el 15% de exposición, procedería a evaluarse qué medida de administración del riesgo incorporar.
Bajo 	<b>No aceptable:</b> Riesgo mayor que 15% y menor o igual que 25%.	Se pasa al siguiente nivel que consiste en definir las opciones de respuesta al riesgo.
Medio 	<b>No aceptable:</b> Riesgo mayor que 25% y menor o igual que 40%.	Se pasa al siguiente nivel que consiste en definir las opciones de respuesta al riesgo, y comunicarlo a la Dirección General Adjunta.
Alto 	<b>No aceptable:</b> Riesgo mayor que 40% y menor o igual que 60%.	Se pasa al siguiente nivel que consiste en definir las opciones de respuesta al riesgo y comunicarlo a la Dirección General y a la Dirección General Adjunta.
Extremo 	<b>No aceptable:</b> Riesgo residual mayor que 60%.	Se pasa al siguiente nivel que consiste en definir las opciones de respuesta al riesgo y comunicarlo a ambas Direcciones y al Consejo Directivo.

**Fuente:** Elaboración propia con base en el programa SIGMA y UNA, 2018.

A raíz de estos criterios, se priorizan los riesgos a tratar, teniendo que, aquellos eventos con niveles de riesgo que se ubiquen en el nivel “aceptable”, no se tratan, pero si se monitorean; mientras que aquellos, con condición de riesgo “bajo”, “medio”, “alto” y “extremo”, es decir, “no aceptables” deberán ser, además de monitoreados, administrados.

## PASO 5. Madurez de las medidas de administración existentes

Los riesgos identificados y valorados deben ser comparados con los controles existentes, es decir, si existen medidas de administración vigentes que regulan los procesos y operaciones habituales de una Unidad y si estas medidas son capaces de afectar los riesgos (contener, tratar, mitigar, etc.). Estos controles deben cumplir con criterios de: “*periodicidad, automatización, aplicación en el proceso y capacidad para minimizar la ocurrencia de un evento*” (INEC, 2017, p.13).

Primeramente, se debe identificar en una lista, los controles existentes que intervienen en el cumplimiento de las actividades de todos los procesos operativos. Seguidamente, se valora la madurez de tales controles. Para este ejercicio, se aconseja el uso de la tabla del **Anexo 5. Matriz para la valoración de la madurez de las medidas administrativas existentes**”, misma que se adjunta como parte de la “*Documentación*” en la respectiva pestaña del SIGMA.

### Etapa 4: Administración de los riesgos

---

Ante aquellos riesgos catalogados como **no aceptables**, se debe determinar las medidas para su tratamiento, y a partir de estas, determinar las Actividades de Respuesta al Riesgo (ARR) dirigidas a su administración; en el entendido de que, el riesgo no se puede evitar ni eliminar del todo, lo que sí resulta posible es su gestión, para el control y reducción de éste. El riesgo se administra a partir de cuatro opciones de respuesta.

Para evaluar y seleccionar la o las medidas de administración con la que se tratarán los riesgos con niveles no aceptables, las jefaturas de Unidad deberán justificar con fundamento en el análisis que realicen al interior de sus procesos, con cuál o cuáles medidas de administración se gestionará el riesgo, o si del todo, no es posible su administración, considerando, entre otros, los siguientes criterios:

- *“la relación costo-beneficio de llevar a cabo cada opción;*
- *la capacidad e idoneidad de los entes participantes internos y externos a la institución en cada opción;*
- *el cumplimiento del interés público y el resguardo de la hacienda pública; y*
- *la viabilidad jurídica, técnica y operacional de las opciones” (D-3-2005-CO-DFOE, CGR, 2005, p.7).*

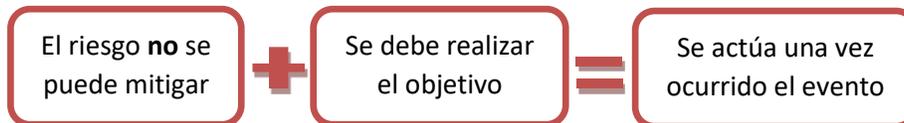
Para efectos de documentación, se sugiere emplear la tabla del **Anexo 6**, instrumento que permite priorizar los riesgos a administrar.

### Opciones de tratamiento del riesgo o medidas para la administración de riesgos

Son los tipos de respuesta que se dan ante aquellos eventos que superan el nivel de riesgo que el ICD ha definido como aceptable.

Opciones de tratamiento sin actividades de respuesta al riesgo:

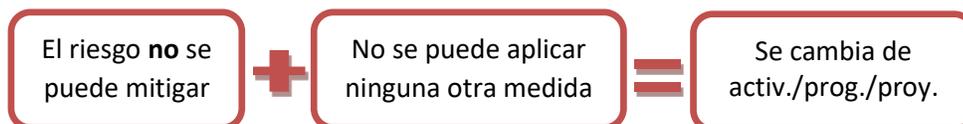
- **Aceptar el riesgo** Es una opción netamente reactiva, pues “*consiste en actuar ante las consecuencias de un evento, una vez que éste ocurra*” (CGR, 2005, p.1). Se reconoce que el objetivo institucional se debe alcanzar, pero también, se reconoce que el riesgo no se puede reducir, evadir o aplicar previamente alguna medida de intervención.



Hay que tener cuidado con esta opción. Ignorar un riesgo es una opción fácil, pero puede desestabilizar, según su magnitud un proceso o la institución. Los riesgos aceptados deben ser objeto de seguimiento y de revisión.

**Ejemplos de riesgos que se aceptan:** Resulta imposible estacionar el vehículo en un parqueo, por lo que se deja en vía pública, ateniéndose al riesgo de que sea tachado o robado; la compra de equipos informáticos de segunda mano con copias piratas de software; y el porcentaje de créditos incobrables que son es considerado "aceptable".

- **Evitar el riesgo** La Administración toma la decisión de no llevar a cabo la actividad, programa o proyecto con el que se pretendía alcanzar el objetivo trazado, no obstante, dicho objetivo se mantiene, pero con otra (s) actividad (es), programa (s) o proyecto (s). (CGR, 2005, p.2). Incluso puede considerarse detener temporalmente el avance del objetivo. Se recurre a esta respuesta, tras considerarse *i)* la madurez de las medidas administrativas existentes; *ii)* que el riesgo es muy elevado; y *iii)* que existen pocas, inviables o nulas alternativas para su mitigación.



**Ejemplos de cambios de actividad/programa/proyecto:** Cancelar una gira y desistir de la construcción de obra pública ante fuertes cuestionamientos de la ciudadanía y medios de comunicación, y otros.

Opciones de tratamiento con actividades de respuesta al riesgo:

- **Modificar el riesgo** Es una opción de carácter preventivo que se da cuando resulta viable la ejecución de actividades para su intervención. Consiste en "*afectar los factores de riesgo asociados a la probabilidad y/o la consecuencia de un evento, previo a que éste ocurra*" (CGR, 2005, p.2). En otras palabras, reducir el riesgo atacando sus causas.



**Ejemplos de ARR:** mantenimiento preventivo, capacitaciones, elaboración de manuales de procedimientos, promover lineamientos, actualizar reglamento, propuesta de ley, campañas de sensibilización ética, establecer un sistema automatizado, boletas de asignación de determinado recurso, revisión contra entrega, generación de reportes mensuales, archivo digital, implementación de medidas de seguridad para los accesos de información (acceso controlado mediante usuario y contraseña, control cruzado -cotejo-, bitácora diaria, etc.), entre otros.

- **Transferir el riesgo** Consiste en que un tercero asuma parcial o totalmente la responsabilidad y/o las consecuencias potenciales de que éste ocurra (CGR, 2005).



**Ejemplos de ARR:** mediante un seguro, se le transfiere la administración de las consecuencias de un riesgo a un tercero (pólizas de fidelidad, seguro de riesgos laborales, seguro de desempleo, etc.), adquisición de almacenamiento de información en la nube, con servicio de soporte y respaldo, para trasladar la información de los servidores institucionales.

*Formulación de Actividades de Respuesta al Riesgo (ARR)*

Las actividades de respuesta al riesgo son aquellas que se requieren implementar para prevenir que el riesgo se materialice sobre los objetivos contenidos en la POSI y en el PNSD. Es la forma en la que se modificará o transferirá el riesgo, lo que implicará la definición de nuevos controles, la mejora de los existentes, la creación de nuevos instrumentos (boletas, guías, otros), la aplicación de medidas de prevención. La intención es cuestionarse sí, con la implementación de dicha ARR, se estaría controlando el riesgo.

A continuación, se presentan a modo de ejemplos, un par de ARR definidas por el Instituto Nacional de Estadística y Censos (INEC) para sus procesos en el 2017:

Riesgo	Nivel de riesgo	Opción de Tratamiento	Control existente sobre el riesgo	ARR Acción de respuesta al riesgo a implementar
Posibilidad de que la documentación archivada en el depósito principal o en los servidores de la Unidad Técnica de Servicios e Informática (UTSI) sufra daños o pérdida.	Medio	Modificar (reducir)	<ul style="list-style-type: none"> <li>*Inventario documental y listas de remisión.</li> <li>*Controles de seguridad contra la extracción no autorizada de documentos (formulario de solicitud, acceso restringido).</li> <li>*El depósito está construido en material inflamable.</li> </ul>	<ul style="list-style-type: none"> <li>*Incluir en el siguiente presupuesto los montos correspondientes para la compra de aires acondicionados para los depósitos documentales.</li> <li>*Llevar a cabo un plan de revisión de las instalaciones y emitir un informe de resultados.</li> </ul>
Posibilidad de que las unidades de marco no cumplan con los criterios para su construcción de acuerdo con la metodología definida.	Alto	Modificar (reducir)	<ul style="list-style-type: none"> <li>*Revisión posterior de las unidades de marco con información recolectada en campo o información de otras fuentes diferentes al Censo.</li> </ul>	<ul style="list-style-type: none"> <li>*Reuniones periódicas con Cartografía para verificar que las construcciones de las unidades de marco cumplen con los requerimientos.</li> </ul>

**Fuente:** Elaboración propia, UPLA, 2018 con base en información del INEC, 2017. Págs. 36 y 38.

Consideraciones:

- Al menos para cada riesgo identificado, debe generarse una ARR.
- Definir los responsables de dar seguimiento a las ARR de cada Unidad (generalmente, son los responsables del nivel de avance y cumplimiento de las metas contenidas en la POSI y los responsables de coordinar la implementación de las iniciativas que operacionalizan las políticas del PNsD).
- El seguimiento de las ARR es semestral. Cada seis meses se definirá y justificará su estado, ya sea si se encuentran implementadas, en proceso de ejecución, sin iniciar o descartadas.
- Las ARR se registran en el SIGMA para su monitoreo y evaluación. Para facilitar su registro, se recomienda completar previamente, la tabla del *Anexo 7. Programación de la actividad de respuesta al riesgo seleccionada para su ejecución*.

#### Etapa 5: Revisión de riesgos

---

En esta etapa, se les dará seguimiento a las actividades de respuesta al riesgo. Es de periodicidad semestral, y se identificará el estado de las ARR, bajo los siguientes parámetros (UNA, 2018):

- **Implementada:** La Unidad informa que la ARR ha alcanzado una ejecución del 100%.
- **En proceso de ejecución:** La Unidad informa que la ARR ha sido cumplida en un % menor al 100%.
- **Sin iniciar:** La Unidad no informa avance y señala que ésta es la razón por la cual no rinde cuentas respecto a ella.
- **Descartada:** La Unidad informa, con la debida justificación, la aparición de condiciones que llevaron a que la ARR perdiera pertinencia y se descartara su ejecución.

#### Etapa 6: Documentación de riesgos

---

Esta etapa es transversal y parte de la identificación, valoración y administración del riesgo, implica tener orden, claridad e incluir el conocimiento de todos los colaboradores. La documentación de riesgos viene a ser el instrumento para que, de *“una forma estructurada [se] asegure su documentación y el control exhaustivo de la información relevante necesaria que dará soporte y en la cual se fundamentarán las siguientes actividades”* (CGR, 2011, p.20).

En el SIGMA, y dentro de algunos módulos, existe una pestaña para adjuntar la documentación de plantillas debidamente cumplimentadas (tablas sugeridas que se pueden consultar en el apartado denominado *“Anexos”* de este documento) y demás, información atinente a la identificación, la valoración y la administración de los riesgos.

## Etapa 7: Comunicación de riesgos

---

Cada jefatura de Unidad tiene la responsabilidad de comunicar los productos intermedios y finales de las etapas del SEVRI a la totalidad de sus funcionarios. El Control Interno, como sistema, se fortalece cuando existe un ambiente que favorece la comprensión del riesgo, la reducción de la incertidumbre, así como, el interés y el compromiso de los funcionarios por sostenerlo y perfeccionarlo.

La Unidad "*Planificación Institucional*", será la instancia asistencial y asesora en el proceso que desarrollará cada Unidad para la identificación, la valoración y la administración de los riesgos. Será la encargada de velar porque cada Unidad del ICD monitoree periódicamente sus riesgos, a fin de realizar la debida evaluación.

Ante una duda sobre el Sistema de Control Interno del ICD, por favor contacte a la Unidad "*Planificación Institucional*", vía telefónica (extensiones 225 y 258) o vía correo electrónico a: [ksegura@icd.go.cr](mailto:ksegura@icd.go.cr) y [dhernandez@icd.go.cr](mailto:dhernandez@icd.go.cr). Además, encontrará información al respecto en la *Intranet institucional*, en la carpeta "*Público*", en la subcarpeta "*Unidad Planificación Institucional*" /Control Interno y SEVRI.

Se recuerda que, es mediante el SIGMA, que se registra y da seguimiento a los datos sobre el control interno y la administración del riesgo institucional, así las cosas, es responsabilidad de cada jefatura y enlace de Unidad mantenerlo actualizado.

## 8. Glosario

Los siguientes términos son extraídos del glosario de las Directrices generales para el establecimiento y funcionamiento del SEVRI, D-3-2005-CO-DFOE de la CGR:

**“Administración de riesgos.** Cuarta actividad del proceso de **valoración del riesgo** que consiste en la identificación, evaluación, selección y ejecución de **medidas para la administración** de riesgos. (*En normativas técnicas esta actividad también se denomina “tratamiento de riesgos”*).

**Actividades de control.** Políticas y procedimientos que permiten obtener la seguridad de que se llevan a cabo las disposiciones emitidas por la Contraloría General de la República, por los jefes y los titulares subordinados para la consecución de los objetivos, incluyendo específicamente aquellas referentes al establecimiento y operación de las **medidas para la administración de riesgos** de la institución.

**Análisis de riesgos.** Segunda actividad del proceso de **valoración del riesgo** que consiste en la determinación del **nivel de riesgo** a partir de la **probabilidad** y la consecuencia de los **eventos** identificados.

**Análisis cualitativo.** Descripción de la **magnitud** de las **consecuencias** potenciales, la **probabilidad** de que esas **consecuencias** ocurran y el **nivel de riesgo asociado**.

**Análisis cuantitativo.** Estimación de la **magnitud** de las **consecuencias** potenciales, de la **probabilidad** de que esas **consecuencias** ocurran y del **nivel de riesgo** asociado.

**Comunicación de riesgos.** Actividad permanente del proceso de **valoración del riesgo** que consiste en la preparación, la distribución y la actualización de información oportuna sobre los **riesgos** a los **sujetos interesados**.

**Consecuencia.** Conjunto de efectos derivados de la ocurrencia de un evento expresado cualitativa o cuantitativamente, sean pérdidas, perjuicios, desventajas o ganancias.

**Documentación de riesgos.** Actividad permanente del proceso de **valoración del riesgo** que consiste en el registro y la sistematización de información asociada con los **riesgos**.

**Estructura de riesgos.** Clases o categorías en que se agrupan los **riesgos** en la **institución**, las cuales pueden definirse según causa de **riesgo**, área de impacto, magnitud del riesgo u otra variable.

**Evaluación de riesgos.** Tercera actividad del proceso de **valoración del riesgo** que consiste en la determinación de las prioridades para la **administración de riesgos**.

**Evento.** Incidente o situación que podría ocurrir en un lugar específico en un intervalo de tiempo particular.

**Factor de riesgo.** Manifestación, característica o variable mensurable u observable que indica la presencia de un **riesgo**, lo provoca o modifica su nivel.

**Identificación de riesgos.** Primera actividad del proceso de **valoración del riesgo** que consiste en la determinación y la descripción de los **eventos** de índole interno y externo que pueden afectar de manera significativa el cumplimiento de los objetivos fijados.

**Magnitud.** Medida, cuantitativa o cualitativa, de la **consecuencia** de un **riesgo**.

**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 de riesgo aceptable.** **Nivel de riesgo** que la institución está dispuesta y en capacidad de retener

para cumplir con sus objetivos, sin incurrir en costos ni efectos adversos excesivos en relación con sus beneficios esperados o ser incompatible con las expectativas de los **sujetos interesados**.

**Parámetros de aceptabilidad de riesgos.** Criterios que permiten determinar si un nivel de riesgo específico se ubica dentro de la categoría de nivel de riesgo aceptable.

**Política de valoración del riesgo institucional.** Declaración emitida por el jerarca de la institución que orienta el accionar institucional en relación con la **valoración del riesgo**.

**Probabilidad.** Medida o descripción de la posibilidad de ocurrencia de un evento.

**Revisión de riesgos.** Quinta actividad del proceso de **valoración del riesgo** que consiste en el seguimiento de los **riesgos** y de la eficacia y eficiencia de las **medidas para la administración de riesgos** ejecutadas.

**Riesgo.** [Es la] **probabilidad** de que ocurran **eventos** que tendrían **consecuencias** sobre el cumplimiento de los objetivos fijados.

**Sistema Específico de Valoración del Riesgo Institucional (SEVRI).** Conjunto organizado de elementos que interaccionan para la **identificación, análisis, evaluación, administración, revisión, documentación** y **comunicación** de los **riesgos** institucionales.

**Valoración del riesgo.** **Identificación, análisis, evaluación, administración y revisión** de los **riesgos** institucionales, tanto de fuentes internas como externas, relevantes para la consecución de los objetivos. *(En normativas técnicas este proceso también se denomina 'gestión de riesgos')*" (CGR, 2005, p.1-3).

## 9. Fuentes consultadas y de referencia

- Asamblea Legislativa (2002) Ley N° 8292, Ley General de Control Interno. Disponible en: <https://cgrfiles.cgr.go.cr/publico/docsweb/portal/documentos/leyes-reglamentos/-8292.PDF>
- Auditoría Superior de la Federación (s.a.) Guía de Autoevaluación de Riesgos en el Sector Público. México. Disponible en: [http://www.oas.org/juridico/PDFs/mesicic5\\_mex\\_ane\\_64.pdf](http://www.oas.org/juridico/PDFs/mesicic5_mex_ane_64.pdf)
- Consejo de Seguridad Vial (2011) Marco orientador del Sistema Específico de Valoración del Riesgo Institucional
- Consejo Nacional de Rehabilitación y Educación Especial (CNREE) (2012) Propuesta: Marco Orientador del Sistema Específico del Riesgo Institucional.
- Contraloría General de la República (2005) Directrices Generales para el establecimiento y funcionamiento del Sistema de Valoración del Riesgo. Disponible en: [http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm\\_texto\\_completo.aspx?nValor1=1&nValor2=55123&nValor3=75419](http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?nValor1=1&nValor2=55123&nValor3=75419)
- Contraloría General de la República (2007) Normas Técnicas para la gestión y el control de las Tecnologías de Información (N-2-2007-CO-DFOE). Disponible en: <https://cgrfiles.cgr.go.cr/publico/docsweb/portal/documentos/manuales-circulares-directrices/N-2-2007-CO-DFOE.DOC>
- Contraloría General de la República (2009) Normas de control interno para el Sector Público, (N-2-2009-CO-DFOE). Disponible en: <https://cgrfiles.cgr.go.cr/publico/docsweb/portal/documentos/manuales-circulares-directrices/nci-publico-N-2-2009-CO-DFOE.PDF>
- Contraloría General de la República (2011) Curso Virtual “Control Interno”. Componente 2: Valoración del Riesgo. Disponible en: [https://www.pgr.go.cr/wp-content/uploads/2017/.../Valoracion\\_del\\_Riesgo\\_teoría.pdf](https://www.pgr.go.cr/wp-content/uploads/2017/.../Valoracion_del_Riesgo_teoría.pdf)
- Contraloría General de la República (s.a.) Curso Modular sobre control interno. Componente 2: valoración del riesgo. Disponible en: [https://www.pgr.go.cr/wp-content/uploads/2017/04/Valoracion\\_del\\_Riesgo\\_teoría.pdf](https://www.pgr.go.cr/wp-content/uploads/2017/04/Valoracion_del_Riesgo_teoría.pdf)
- Contraloría General de la República. (2005) Directrices generales para el establecimiento y funcionamiento del sistema específico de valoración del riesgo institucional D-3-2005-CO-DFOE. Disponible en: <https://cgrfiles.cgr.go.cr/publico/docsweb/documentos/control-interno/directrices-sevri.doc>
- Devment, M. (2013) Factibilidad de sistemas: Técnica, Económica y Operativa. Disponible en: <http://www.atic.cl/factibilidad-de-sistemas/>
- Equivida. (s.a.) Riesgos personales. Tomado de: <https://www.equivida.com/tipos-de-riesgo>

INEC (2017) Informe de la implementación del Sistema Específico de Valoración del Riesgo en el Instituto Nacional de Estadística y Censos, 2016. Disponible en: [http://www.inec.go.cr/sites/default/files/documentos-biblioteca-virtual/informe\\_de\\_la\\_implementacion\\_del\\_sevri\\_en\\_el\\_inec\\_05052017\\_v3.pdf](http://www.inec.go.cr/sites/default/files/documentos-biblioteca-virtual/informe_de_la_implementacion_del_sevri_en_el_inec_05052017_v3.pdf)

Instituto Nacional de Estadística y Censos (2017) Generalidades del Sistema de Control Interno Unidad de Planificación Institucional. Disponible en: <http://www.inec.go.cr/sites/default/files/documentos-biblioteca-virtual/cigeneralcontrolupi2017.pdf>

ICD (2011). Política de Gestión de Riesgo Institucional y parámetros de aceptabilidad. Acuerdo número ciento cuarenta y dos-cero ocho-dos mil once, tomado en la Sesión Ordinaria Número Ocho, catorce de noviembre del dos mil once. Consejo Directivo. Disponible en: Plataforma SIGMA, ICD-Portal.

Ministerio de Salud (2008) Directriz DM-EC-3035-08. Disponible en: <https://cgrfiles.cgr.go.cr/publico/jaguar/USI/.../DIRECTRIZ-DM-EC-3035.doc>

Ministerio de Seguridad Pública (2012) Metodología SEVRI-MSP conforme al marco orientador y políticas específicas para la gestión integral del riesgo institucional. MSP-OMCGI-UGR-MSEVRI-MSP-02-2012. Disponible en: <http://www.seguridadpublica.go.cr/funcionarios/sevri/UGR%20Guia%20Metodologica%20SEVRI-MSP%202013.pdf>

MTSS (2016) Informe de Valoración de Riesgos Institucionales 2016. San José, Costa Rica

Oxford University Press (s.a.) Diccionario Oxford en línea (Oxford Dictionaries: Spanish Dictionary & Translations). Disponible en: <https://es.oxforddictionaries.com/definicion/>

Registro Nacional (2017) Sistema Específico de Valoración del Riesgo Institucional 2017. 6ta edición.

Servicio Nacional de Salud Animal (2015) Sistema Específico de Valoración del Riesgo Institucional SEVRI. SENASA.

Universidad Monteávila (S.f.) Factibilidad Técnica y Operacional. Aula Virtual UMA. Curso de Especialización en Planificación, Desarrollo y Gestión de Proyectos. Disponible en: [https://www.uma.edu.ve/moodle\\_uma/course/info.php?id=28](https://www.uma.edu.ve/moodle_uma/course/info.php?id=28)

Universidad Nacional (2018) Metodología del Sistema Específico de Valoración de Riesgo Institucional de la Universidad Nacional (Sevri- UNA) Área de Planificación, Sección de Control Interno. Disponible en: [http://documentos.una.ac.cr/bitstream/handle/unadocs/9198/Metodologia%20Sevri\\_UNA.doc?sequence=1&isAllowed=y](http://documentos.una.ac.cr/bitstream/handle/unadocs/9198/Metodologia%20Sevri_UNA.doc?sequence=1&isAllowed=y)

## 10. Anexos

### Anexo 1. Técnicas para la identificación y el análisis del riesgo institucional

<i>Técnica</i>	<i>Concepto</i>
1. Talleres. 2. Lluvia de Ideas.	<ul style="list-style-type: none"><li>• La primera técnica implica realizar reuniones que incluyan personal de diferentes niveles relacionados con los fines de la Unidad.</li><li>• En caso de no ser posible la realización de un taller, se puede emplear la segunda técnica con grupos más pequeños a nivel de Unidad.</li></ul> En ambos casos, el ejercicio consiste en identificar, analizar y evaluar riesgos, y plantear posibles opciones de respuesta (cómo tratarlos).
3. Mapeo de procesos.	Aquellos procesos que cuenten con una clara identificación (y documentación) de la secuencia (cada paso) de las etapas, acciones o actividades que integran sus procesos, pueden emplear esta técnica que permitirá identificar los puntos críticos a lo largo del proceso, que presenten o puedan presentar riesgos.
4. Análisis del entorno interno y externo.	Implica considerar qué cambios en marco legal, en la realidad económica, política, social, o cualquier otra, pueda hacer peligrar el alcance de los objetivos.
5. Encuestas. 6. Entrevistas.	Por medio de alguna de estas dos técnicas, se realiza una serie de preguntas a mandos medios y altos, dirigidas a identificar y analizar los riesgos.
8. Análisis comparativo.	Se identifican riesgos de la propia institución, basándose en un análisis de otras entidades del sector que tengan una misma razón de ser, o traten temáticas similares.

**Fuente:** Elaboración propia con base en ASF, s.a. 2018.

**Anexo 2.** Listado de categorías de riesgos institucionales del ICD.

Tipo	Definición	Subtipo	Definición
1. Riesgos operativos	Riesgo presente en la cotidiana y normal ejecución de los procesos, actividades y tareas de un ente. Implica fallas con los productos o servicios que se brindan. En otras palabras, es el riesgo de que <i>"la puesta en marcha de la política Institucional esté condicionada por procesos y procedimientos inadecuados"</i> (MTSS, 2016, p.20).	1.1. Procesos y controles inadecuados, insuficientes o ausentes.	Se da cuando se carece de una revisión de los procesos y controles para detectar fallas, debilidades y necesidades, por ejemplo: proceso de documentación institucional con vacío en los controles, proceso de almacenamiento de bienes sin la actualización y automatización debida, etc.
		1.2. Uso inapropiado e ineficiente de recursos.	Se presenta cuando hay una deficiente distribución de los recursos, donde hay programas y proyectos sin respaldo presupuestario, mientras que otros, despilfarran o subutilizan los recursos asignados a la entidad.
		1.3. Riesgos de información operativa	Se refiere a la información relacionada con aquellos elementos que intervienen en la formulación e implementación de acciones operativas.
		1.4. Alineamiento operativo-estratégico (desvinculación o asocie incorrecto)	Consiste en <i>"(...) no alinear los objetivos de los procesos de la institución y las medidas de desempeño con [planes,] objetivos y estrategias, puede producir actividades antagónicas y descoordinadas en toda la institución"</i> (MSP, 2012, p.46).
		1.5. Eficiencia	Son aquellas <i>"Operaciones ineficientes [que] amenazan la capacidad de proporcionar los servicios a costos razonables para asegurar los productos esperados por la población en forma oportuna"</i> (MS, 2008, p.8).
		1.6. Capacidad instalada	Sucede cuando la <i>"Capacidad instalada insuficiente amenaza la habilidad de la institución para cubrir las demandas de los habitantes"</i> . (MS, 2008, p.8).
		1.7. Riesgo de oportunidad	Se refiere a <i>"un plazo excesivo entre el inicio y el término de un proceso"</i> (MTSS, 2017, p.7), lo que puede provocar la pérdida de oportunidades.

Tipo	Definición	Subtipo	Definición
2. Riesgos financieros	En el manejo de los recursos financieros, existe la posibilidad de que los flujos de ingresos y activos financieros no se manejen de una forma eficiente y efectiva que maximice su disponibilidad y uso racional (CSV, 2011).	2.1. Alineamiento presupuestario (Desvinculación / asocie incorrecto)	Consiste en no alinear el presupuesto con los planes y los objetivos estratégicos y operativos sustantivos, puede provocar atraso en los objetivos planteados. La desvinculación acarrea errores en la ejecución (asignación no óptima o que no cubre las necesidades reales), y afecta el seguimiento y la evaluación de los resultados. También se origina "(...) <i>por controles insuficientes, deficientes o ausentes, [que] el presupuesto no se administre bien e impida alcanzar los objetivos y las metas [organizacionales]</i> " (MS, 2008, p.9).
		2.2. Instrumentos financieros	Este riesgo conlleva la exposición a costos de administración excesivos o pérdidas, debido a la complejidad o a las consecuencias imprevistas sobre los instrumentos financieros adquiridos (MS, 2008).
		2.3. De liquidez (afectación del flujo de efectivo)	Refiere a la limitación de no contar oportunamente con efectivo, es un riesgo que conlleva el incumplimiento de las obligaciones asumidas por la institución (MS, 2008).
		2.4. Transferencias	Consiste en la transferencia de fondos con debilidades, las que pueden derivar en pérdidas económicas, así como, en el incumplimiento de funciones u objetivos (MS, 2008).
		2.5. De garantía	Es la "(...) <i>pérdida parcial o total del valor de un activo dado en garantía, expone al [ICD] a una pérdida financiera</i> " (MS, 2008, p.8).
		2.6. De determinación de costos	Refiere a un inadecuado o inexistente análisis de costos que "(...) <i>puede resultar en gastos excesivos e injustificados, no congruentes con la calidad de los servicios</i> " (MS, 2008, p.9).
		2.7. Asignación de recursos	Es un proceso de asignación de recursos, de adquisición de bienes y servicios e información de soporte inadecuados que atenta contra el logro de los objetivos organizacionales.

Tipo	Definición	Subtipo	Definición
3. Riesgos de recurso humano	Son riesgos derivados de la disponibilidad, calidad, conocimientos, habilidades, experiencias y capacitación de los funcionarios. Se pueden materializar al existir la "posibilidad de no seleccionar, motivar, ubicar y orientar a los recursos humanos para el logro de los objetivos" (MTSS, 2015, p.7) del ICD. Estos riesgos también se pueden asociar a la eficiencia y a la eficacia del desempeño de los funcionarios, el desarrollo de estos y el ambiente laboral en el que se desenvuelven.	3.1. Gestión del recurso humano	Es el riesgo de genera "(...) una inapropiada planificación, selección, motivación, ubicación, formación y evaluación del personal, para el logro de los objetivos..." (SENASA, 2015, p.21) institucionales. Por ejemplo: insuficiencia de plazas y el consecuente recargo de funciones o abandono de estas.
		3.2. Capital de conocimiento	Refiere a los procesos de acumular, acrecentar e institucionalizar el conocimiento, cuando son ineficaces, limitados o inexistentes "(...) produciendo un tiempo de respuesta lento, costos altos, errores repetidos, lento desarrollo de competencias, restricciones en el crecimiento y empleados desmotivados"(MS.2008. p.8).
		3.3. Desempeño	Es la posibilidad de que el desempeño del personal se vea limitado por factores de eficiencia, eficacia y aptitudes de estos.
		3.4. Riesgos de salud ocupacional	Son aquellos riesgos laborales como los higiénicos, de exposición a sustancias tóxicas, de exposición a accidentes, de poca iluminación, de exceso de ruido, de sobrecarga física, mental y social. A estos, se suman los ergonómicos como el espacio y las condiciones de trabajo, en el tanto, afecten directa, periódica o estructuralmente el alcance de los objetivos institucionales.  También se considera la posibilidad de que exista o se genere un clima inadecuado para el desempeño laboral, y que haya políticas de rendimiento y compensación para el personal inapropiadas o inexistente.

Tipo	Definición	Subtipo	Definición
4. Riesgos tecnológicos y de información	<p>Los riesgos de información son aquellos asociados a la calidad, la cantidad, los medios de transmisión y la custodia de esta cuando se afectan las transacciones, operaciones y toma de decisiones de la organización. (SENASA, 2015). Estos riesgos se pueden dar cuando:</p> <ul style="list-style-type: none"> <li>-la capacidad institucional, no es suficiente para atender las necesidades de desarrollo y soporte tecnológico;</li> <li>-las tecnologías no operan dentro de lo esperado;</li> <li>-cuando se violenta la integridad y la confiabilidad de la información/datos; y</li> <li>-no se da el soporte adecuado a los procesos de trabajo de las Unidades (MTSS, 2016).</li> </ul>	4.1. Disponibilidad de la información	Consiste en la "(...) <i>no disponibilidad de información cuando se le necesita, amenaza la continuidad de las operaciones y procesos institucionales</i> " (MS, 2008, p.9). Por ejemplo: interrupciones del servicio y ausencia de respaldos de información.
		4.2. Infraestructura tecnológica	Es el riesgo de que la institución no cuente con los recursos necesarios como son: el hardware-equipos, las redes, el software, procesos claramente identificados, personal especializado, etc.; mismos que permiten sostener los procesos operativos y dar soporte eficaz a los requerimientos de información de la entidad, actuales y futuros (MS, 2008).
		4.3. Entorno información seguro y protegido	Es la probabilidad de que no se disponga de la información bajo criterios de integridad, confiabilidad, acceso y disponibilidad que sustente la toma de decisiones en los diferentes procesos. Implica "(...) <i>la existencia de sistemas de control mal diseñados e información dudosa, que faciliten el fraude y amenace la integridad de los sistemas</i> " (Senasa, 2015, p.).
		4.4. Tecnología de apoyo a la toma de decisiones	Refiere a la carencia de un sistema integrado de gestión y/o una base de datos unificada, actualizada de acceso institucional que facilite los procedimientos y la toma de decisiones (MTSS, 2015). Otros riesgos pueden ser la existencia de procesos manuales, poco automatizados, que conllevan pérdida de confiabilidad, de calidad y de seguridad de los datos.
		4.5. Almacenaje de información	Consiste en la probabilidad de que sucedan eventos o situaciones que generen pérdida de información por uso, manejo y archivo inadecuado de esta. También refieren al incumplimiento de políticas en cuanto al manejo de la información necesaria para la toma de decisiones. (Senasa, 2015).
		4.6. Comunicación de la información	Es la ocurrencia de situaciones de riesgo por el uso de canales ineficientes e inadecuados de comunicación que pueda distorsionar la información, o bien, el suministro de esta por parte de funcionarios (Senasa, 2015).

Tipo	Definición	Subtipo	Definición
5. Riesgos jurídicos	Son riesgos que facilitan la "(...) transgresión del principio de legalidad. Refiere a la cantidad y a la magnitud de cambios (variabilidad)..."(MTSS, 2015) de la legislación que afecten funciones, así como, el logro de objetivos.	5.1. Cumplimiento	Consiste en el incumplimiento de las políticas y los procedimientos organizacionales, leyes y regulaciones, generando así baja calidad en los productos, retrasos innecesarios, penalidades, multas, etc. (MS, 2008).
		5.2. Desactualización / imprecisiones de la normativa	Refiere a la desactualización e imprecisiones de la normativa en términos de funciones, ámbitos de acción y otros, que limitan la labor institucional y su naturaleza rectora: <ul style="list-style-type: none"> <li>-Normativa vinculada al fenómeno de las drogas, actividades conexas, entre otros delitos asociados;</li> <li>-normativa en materia de contratación administrativa;</li> <li>-normativa presupuestaria;</li> <li>-normativa laboral;</li> <li>-protección y tratamiento de información y procedimientos;</li> <li>-diferencias de criterios jurídicos; e</li> <li>-incertidumbre y/o incapacidad de cumplir con las obligaciones y respetar los derechos jurídicos o reglamentarios; entre otros.</li> </ul>

Tipo	Definición	Subtipo	Definición
6. Riesgos de dirección	Es el riesgo de que tanto los titulares como sus subordinados, sean mal dirigidos o excedan los límites de sus responsabilidades, es el problema de competencias mal definidas, que terminan generando conflictos internos, extralimitación en la actuación u omisiones entorno al cumplimiento de funciones (MTSS, 2015), es decir, que los funcionarios no sepan qué hacer o se excedan en su actuación, violentando los límites de la autoridad formal de la organización.	6.1. Liderazgo de la dirección y las jefaturas	Se da cuando los funcionarios de la institución no son liderados con eficacia, lo que puede derivar en una ausencia de: pérdida de enfoque centrado en el usuario o problema a solucionar, de motivación, de credibilidad y de pérdida de confianza/legitimidad en la dirección (MS, 2008).
		6.2. Capacidad de gestión y planificación	Refiere a la eventual incapacidad de la Unidad u Órgano para cumplir con sus responsabilidades, evidenciando con ello fallas en la dirección. También tiene que ver con la capacidad instalada para producir el bien o servicio, amenazando con ello el cumplimiento de los objetivos identificados" (SENASA, 2015), así como, la previsión mediante la planificación, de las necesidades reales y potenciales, y la capacidad de respuesta institucional.
		6.3. Liderazgo del ICD como ente rector	Se da cuando la institución no lidera de manera efectiva a las instancias ejecutoras y operadoras de políticas estatales en materia de drogas, actividades conexas y delitos asociados, por una falta de conducción adecuada para el logro de los objetivos trazados en el marco de las citadas políticas (MS, 2008).
		6.4. Competencias internas y límites de autoridad	Se da como resultado de una inadecuada definición y/o verificación de los límites del accionar de cada dependencia, jefatura y funcionario, causando así: -Conflictos internos por actos no autorizados o no éticos; -que se asuman riesgos no autorizados o inaceptables; -que se evada la responsabilidad por los actos realizados; y -extralimitación u omisión de funciones entre unidades, órganos staff y direcciones (MS, 2008).
		6.5. Coordinación técnica y administrativa entre dependencias que intervienen en un mismo proceso/actividad/etc.	Sucede cuando las Unidades y Órganos staff de la entidad trabajan de manera aislada e independiente, con mínima o nula coordinación para la consecución de objetivas y metas definidas en el marco de programas, proyectos o procesos organizacionales, nacionales e internacionales. También puede darse cuando se carece de visión sistémica, donde cada Unidad es un subsistema de un proceso mayor (finalidad), que requiere de la articulación de todos sus engranajes (Unidades).

Tipo	Definición	Subtipo	Definición
7. Riesgos estratégicos y de gestión	Se refiere a "las condiciones que disminuyen la capacidad de los directivos, de implementar efectivamente la estrategia de la Institución. Se enfoca en asuntos globales relacionados con la Misión y el cumplimiento de los objetivos estratégicos, claridad en las políticas, diseño y conceptualización de la organización" (RN, 2017, p.23).	7.1. Monitoreo del entorno	Es cuando la ausencia de monitoreo del entorno o la formulación de supuestos poco realistas o erróneos sobre los riesgos del entorno puede causar que se prosigan con estrategias obsoletas o ineficaces (MS, 2008).
		7.2. Medición de indicadores de gestión e impacto	Sucede por la existencia de indicadores de gestión e impacto poco relevantes, nada confiables e inconsistentes con las estrategias establecidas, amenazando con ello (MS, 2008, p.10) la capacidad del ICD para responder exitosamente a su competencia jurídica y política.
		7.3. Planificación	Refiere a un proceso de planificación estratégica poco riguroso técnica y metodológicamente, con escasa participación de distintos actores (políticos y técnicos) y sectores (gubernamentales y no gubernamentales), lo que conduce a la generación de un producto sesgado, carente de legitimidad, pobre en información, condicionantes indispensables para la generación de estrategias efectivas, con debilidades desde el inicio para su materialización, seguimiento y evaluación.
		7.4. Riesgos de información para la toma de decisiones	Son aquellos que se desprenden de la posibilidad de que la información necesaria para la ejecución de: i) la programación estratégica y operativa-sustantiva; y ii) el seguimiento y la verificación de la calidad de la gestión e impacto institucional, no sea relevante o confiable.  Afecta también, la rendición de cuentas institucional, nacional e internacional. Este tipo de riesgo se puede presentar en todos los esfuerzos y actividades que crean valor, aquellas que procuran la satisfacción de las necesidades de la población interna y externa al Instituto (MS, 2008).
		7.5. Alineamiento estratégico	Consiste en la posibilidad "(...) de que la visión del nivel jerárquico superior no sea compatible con las competencias institucionales" (SENASA, 2015, p.21).

Tipo	Definición	Subtipo	Definición
8. Riesgos de integridad	Son aquellos riesgos que posibilitan la planificación y ejecución de acciones vinculadas a actos corrupción, fraude, ilegalidad y otras irregularidades que atentan contra los deberes de los funcionarios, y que terminan, afectando el cumplimiento de objetivos institucionales; es decir, refiere a "la realización de actos ilegales y actos no autorizados, los cuales podrían resultar en la pérdida de la imagen institucional" (MSP, 2012, p.45).	8.1. Corrupción	Refiere al "uso indebido de funciones y recursos públicos para obtener o conceder beneficios personales, políticos, o de terceros, en contravención de las disposiciones legales y la normativa" (RN, 2017, p.23)
		8.2. Fuga de información	Consiste en la salida no controlada de información a terceros no autorizados o en la que, el responsable de esta, pierde su control, además de atentar contra el alcance de los objetivos, lo que implicaría una pérdida de imagen institucional y de credibilidad, por parte de otras entidades hacia el ICD.
		8.3. Riesgos de imagen institucional	La imagen institucional es un elemento clave para toda organización. Si esta es percibida positivamente por sus usuarios y el público, crece el nivel de confianza y se fortalecen las relaciones de cooperación interinstitucionales e intersectoriales.
		8.4. Falta al deber de probidad	Refiere a la violación del deber de probidad, es decir, cuando "(...) la conducta de funcionario debe apegarse en todo momento a postulados de transparencia, rendición de cuentas, honradez, rectitud, respeto, discreción, integridad, imparcialidad, lealtad, espíritu de servicio, buena fe, etc. (...)" (Procuraduría General de la República, 2016).  ¿Qué es probidad? La probidad es la aplicación de honestidad, rectitud, honradez, responsabilidad y la ética en el puesto en que se desempeña la persona (Fabrizio Montero, 2018).

Tipo	Definición	Subtipo	Definición
9. Riesgos del entorno	Son aquellos riesgos que se relacionan con factores externos a la organización, con la capacidad actual o futura de incidir negativamente en el cumplimiento de los objetivos, las metas y la estrategia institucional y/o nacional.	9.1. Capacidad de adaptación al entorno	Se da cuando el personal de la institución no puede implementar mejoras en los procesos y servicios en los que participa, lo suficientemente rápido para responder a los cambios del entorno.
		9.2. Entorno político externo	Son aquellos que se relacionan con las decisiones políticas de los Poderes Ejecutivo, Legislativo y Judicial, que afectan el ámbito de acción, el presupuesto, las estrategias, los programas, los proyectos, entre otros, del ICD.
		9.3. Entorno jurídico externo	Refiere a cualquier situación, actual o eventual, a nivel normativo, que no se haya considerado dentro de la categoría "5. Riesgos jurídicos" y que se desprenda de un análisis del entorno.
		9.4. Entorno económico externo	Es aquél, cuyos factores inciden en el comportamiento del mercado, cambios en la demanda y en la oferta, cambios sobre variables macroeconómicas, entre otras opciones.
9. Riesgos del entorno		9.5. Entorno sociocultural externo	Son aquellos riesgos que surgen ante fenómenos y fuerzas socio-culturales (antagónicas, resistentes, coyunturales, estructurales, comunales, regionales, etc.) que alteran el comportamiento de las variables sociales sobre las que el ICD trabaja, incidiendo así, sobre el logro de los objetivos institucionales.
		9.6. Relaciones intersectoriales e interinstitucionales	Refiere a la ausencia o debilidad en la coordinación interinstitucional, intersectorial, omisión de amenazas y oportunidades para gerenciar la rectoría institucional en materia de drogas, actividades conexas y delitos asociados; y a la no identificación de posibles conflictos de competencias y oportunidades de alianzas.
		9.7. Entorno de innovación tecnológica	Consiste en la posibilidad de que los avances en materia tecnológica que demanda el país, la normativa vigente, las organizaciones dedicadas a la criminalidad organizada, etc.; no estén acordes con la realidad institucional.

<i>Tipo</i>	<i>Definición</i>	<i>Subtipo</i>	<i>Definición</i>
		9.8. Entorno ambiental	Son aquellos fenómenos naturales o provocados por el ser humano que conducen a una catástrofe o daño, y que ante la falta de previsión institucional, la consecución de los objetivos institucionales se ve negativamente afectada.
10. Otros		10.1. Riesgos de infraestructura	Se dan cuando se carece de infraestructura necesaria para la normal actividad institucional, así como, para la generación de los servicios, afectando de esta manera, la satisfacción de las necesidades y requerimientos de la población a la que se destinan los esfuerzos.
		10.2. Otros	Cualquier otro riesgo que no se puede establecer dentro de alguna de las clasificaciones anteriores.

**Fuente:** Elaboración propia con base en MTSS, 2016; CNREE, 2012; CSV, 2011; RN, 2017; SENASA, 2015; MS,2008, MSP, 2012 y SIGMA-ICD, 2012.

**Anexo 3.** Matriz para la identificación del riesgo institucional, según procesos y objetivos de la POSI

<b>Matriz para la identificación del riesgo institucional, según procesos y objetivos de la POSI</b>										
										dd/mm/aa
Unidad:					Fecha de elaboración:					
Proceso	Código del objetivo	Objetivo	Código del riesgo	Nombre del riesgo	Descripción del riesgo	Tipo de riesgo	Subtipo de riesgo	Causa	Consecuencia	Priorización ¿Prioritario o no? Asignar un valor de 1-10

Fuente: Elaboración propia con base en ASF, s.a. 2018.

**Anexo 4.** Matriz para la valoración del riesgo institucional, según procesos y objetivos de la POSI

<b>Matriz para la valoración del riesgo institucional, según procesos y objetivos de la POSI</b>										
									dd/mm/aa	
Unidad:					Fecha de elaboración:					
Proceso	Código del objetivo	Objetivo	Código del riesgo	Nombre del riesgo	Descripción del riesgo	Probabilidad	Impacto	Nivel de exposición al riesgo	Nivel de riesgo	

Fuente: Elaboración propia con base en ASF, s.a. 2018.

**Anexo 5. Matriz para la valoración de la madurez de las medidas administrativas existentes**

<b>Matriz para la valoración de la madurez de las medidas administrativas existentes</b>										
										dd/mm/aa
Unidad:					Fecha de elaboración:					
Proceso	Código del objetivo	Objetivo	Tareas/ actividades del objetivo	Medida existente para esa actividad	Valoración					
					No existe (0)	Deficiente (1)	Regular (2)	Bueno (3)	Muy bueno (4)	Excelente (5)
Gestión financiera contable: Contabilidad			Liquidación presupuestaria	Revisión de la documentación al recibir los pedidos.					4	
				Verificación del comprobante con visto bueno técnico.				3		
				Control de entrega digital.			2			
Planificación operativa			Seguimiento a proyectos	Reportes trimestrales de cambios de límites.					4	
				Acta de constitución del proyecto e inventario de entregables.	0					

**Fuente:** Elaboración propia, UPLA, 2018 según SIGMA y UNA, 2018.

Al asignar a cada medida, una valoración, esta debe responder a: *i)* ¿es un instrumento que requiere de una actualización regular?, y si es así, ¿se renueva con periodicidad?; *ii)* ¿la medida es manual, engorrosa o se ha logrado su automatización?; *iii)* ¿está sólidamente instaurada dentro de las medidas que se toman, o queda a criterio de cada quien bajo qué circunstancias, y cómo usarla?; *iv)* ¿permite consultar resultados y registros con rapidez, seguridad y confiabilidad?; *v)* ¿se aplica actualmente para lo que fue diseñada, ocasionalmente, o bien, existe, pero sin ser empleada?; *vi)* ¿este control es capaz de reducir la incidencia o materialización de un evento de riesgo?; *vii)* es de carácter preventivo, correctivo o de detección; y *viii)* entre otros.

En caso de que no se cuenten con medidas, la valoración será de 0.

**Anexo 6.** Matriz para la priorización de los riesgos institucionales a administrar

<i>Matriz para la priorización de los riesgos institucionales a administrar</i>												
Unidad: <input type="text"/>											dd/mm/aa	
											Fecha de elaboración: <input type="text"/>	
Código del riesgo	Nombre del riesgo	Nivel de exposición	Grado de madurez de las medidas administrativas existentes	Criterio de aceptación	Nivel de riesgo	Criterios de priorización						Total (priorización)
						Costo/beneficio	Capacidad e idoneidad	Interés público	Viabilidad jurídica	Viabilidad técnica	Viabilidad operativa	
010		10%	-4	Aceptable								
004		45%	0	Alto								
016			-1	Medio								
001			-3	Aceptable								
008		<b>60%</b>	-2	Extremo								

Fuente: elaboración propia, UPLA, 2018.

En la página siguiente, indican las instrucciones sobre cómo completar la matriz.

La tabla se completa desde una plantilla en Excel. Los primeros cinco componentes (“*código del riesgo*”, “*nombre del riesgo*”, “*nivel de exposición*”, “*madurez de las medidas administrativas existentes*” y “*criterios de aceptación*”) se toman de las tablas trabajadas en las etapas anteriores. Con respecto a la sección “*criterios de priorización*” de las ARR, estos, responden a las consideraciones que establece la CGR. Es conveniente que cada Unidad, conforme un equipo evaluador para asignar una puntuación conforme a las consideraciones que se enlistan párrafos de abajo.

La sumatoria de estas puntuaciones dará un total por cada ARR, de tal forma que aquellas ARR que: **i)** corresponden a riesgos con criterio “*No aceptable*”; **ii)** cuenten con viabilidad jurídica; y **iii)** obtengan mayores puntajes, serán las que se seleccionen para la administración de su respectivo riesgo y, a su vez, se incorporen en el SIGMA para su documentación. Esta plantilla se adjuntará en la pestaña “Documentación” del SIGMA para efectos de registrar el ejercicio de priorización de las ARR.

Aquellos riesgos con criterio “*No aceptable*” y de exposición “*Alta*” y “*Extrema*”, cuyas ARR obtengan una priorización baja (valor bajo en la columna “*Total (priorización)*”), lo que los dejaría por fuera de ejecutar ARR’s que los traten), debido a costos altos, inviabilidad, y limitaciones de capacidad e idoneidad; precisarán, repetir el ejercicio de pensar en una o más ARR alternativas, que sean sometidas, a su vez, a la valoración por el equipo evaluador, sobre su priorización, con la finalidad, de que estos riesgos no aceptables, de alta y extrema exposición no dejen de ser atendidos.

A continuación, se sugieren consideraciones para que el equipo evaluador, analice y calcule cada factor de priorización de la tabla del **Anexo 6**:

- **Costo/Beneficio:** consiste en estimar si el costo de implementar ARR es menor o mayor que el costo de no implementarlas y que acontezca el evento de riesgo y afrontar sus consecuencias. Esta decisión se basa en el uso eficiente y razonable de los recursos públicos, es decir, considera como criterio el resguardo de la hacienda pública.

Tal y como lo define la CGR, para aquellos riesgos con criterio “*No aceptable*”, debe considerarse que, si se ubican:

- “*en la categoría de nivel de riesgo bajo y medio serán “aceptables” si los costos de su administración exceden los beneficios o son imposibles de administrar por vías distintas (...)*” (CGR, s.a. p.26) a la opción de tratamiento: aceptar el riesgo, es decir, atenerse a las consecuencias.
- “*en la categoría de nivel de riesgo alto son aceptables únicamente bajo circunstancias extraordinarias justificadas*” (CGR, s.a. p.26).

Se asigna un valor del 1 al 5. Entre menor sea el costo de las ARR con respecto a las consecuencias de materializarse el evento, más alto es este indicador (5), entre mayor sea el costo, más bajo es su valor (1).

- **Capacidad & Idoneidad:** Refiere a la capacidad e idoneidad de los actores tanto internos como externos de la organización, específicamente, al “*grado en que la institución puede*

*afectar los factores de riesgo, es la posibilidad que tiene la institución de influir sobre los riesgos, en sus causas o consecuencias” (CGR, s.a. p.25). Según la naturaleza, complejidad y recurrencia del evento de riesgo, se determina si, el ICD y/o entes que estén relacionados se encuentran en capacidad de dar respuesta y son los adecuados para tratar el mismo.*

Se asigna un valor del 1 al 5. Entre mayor capacidad e idoneidad cuenta el ICD y/u otros entes, más alto es este indicador (5), entre menor capacidad e idoneidad se estime, más bajo es su valor (1).

- **Interés Público:** Refiere a la *“importancia de la política, proyecto, función o actividad afectados”* (CGR, s.a. p.25) y al cumplimiento del interés público.

Se asigna un valor que oscila entre 1 y 5. Entre mayor sea la importancia del objetivo de la POSI de una Unidad, más alto es este indicador (5), entre menor sea la importancia de dicho objetivo, más bajo es su valor (1).

- **Viabilidad Jurídica:** Refiere a la viabilidad jurídica de la ARR que se defina para tratar el riesgo. Responde a las preguntas: *i) ¿se cuenta con respaldo de la normativa vigente para implementar la ARR?; y ii) ¿la ARR que se piensa desarrollar posee restricciones de carácter legal?*

La viabilidad jurídica siempre tiene que darse, por lo tanto, se selecciona "Sí", si la ARR cuenta con viabilidad jurídica y "No", si es inviable. Si se selecciona "No", automáticamente la ARR no se prioriza, pues es una acción que, al no contar con sustento legal, no puede ser implementada. Así las cosas, exige su descarte y demanda el replanteamiento de la alternativa de la ARR para administrar el riesgo.

- **Viabilidad Técnica<sup>4</sup>:** Refiere a la viabilidad técnica de la ARR que se defina para tratar el riesgo. Procura responder a preguntas como: *i) ¿la ARR a implementar será eficiente, eficaz, pertinente y sostenible durante el tiempo que requiere el riesgo para ser tratado?; ii) ¿es posible su funcionamiento?; y iii) ¿existen las condiciones administrativas, de infraestructura, ambientales, tecnológicas, etc., necesarias para su concreción y mantenimiento?*

Se asigna un valor que oscila entre 1 y 5. Entre mayor viabilidad técnica se estime, más alto es este indicador (5), entre menor viabilidad, más bajo es su valor (1).

- **Viabilidad Operativa<sup>5</sup>:** Refiere a la viabilidad operativa de la ARR que se defina para tratar el riesgo. Entre otros cuestionamientos, puede plantearse si: *i) ¿existen las capacidades organizacionales para implementar y sostener la ARR?; ii) ¿se cuenta con el recurso humano y las posibilidades de capacitación para su operacionalización?; iii) ¿facilita el logro del*

---

<sup>4</sup> Basado en Devment, M. (2013) y Universidad Monteávila (S.f.).

<sup>5</sup> Basado en Devment, M. (2013) y Universidad Monteávila (S.f.).

objetivo, o por el contrario, lo limita o traba?; y iv) ¿la ARR podría ser compleja, no contar con el apoyo de los funcionarios, requerir de un proceso de adaptación intenso y/o extenso?

Se asigna un valor que oscila entre 1 y 5. Entre mayor viabilidad operativa se estime, más alto es este indicador (5), entre menor viabilidad, más bajo es su valor (1).

**Anexo 7.** Programación de la actividad de respuesta al riesgo seleccionada para su ejecución

<b>Programación de la actividad de respuesta al riesgo seleccionada para su ejecución</b>							
<b>Proceso:</b>						<b>Fecha elaboración:</b>	
<b>Objetivo:</b>						<b>Responsable:</b>	
<b>Riesgo:</b>						<b>Cód. del riesgo</b>	
<b>ARR #1:</b>						<b>Costo anual estimado:</b>	
Tarea / actividad a realizar	Fecha inicio dd/mm/aa	Fecha fin dd/mm/aa	Porcentaje de avance				Estado: Implementada, en proceso, sin iniciar, descartada.
			25%	50%	75%	100%	
<b>Estado general de la ARR:</b>							

Fuente: Elaboración propia, UPLA, 2018 con base en MSP, 2012, p.38.