|  |  |
| --- | --- |
| Logotipo  Descripción generada automáticamente  | **PODER JUDICIAL**  |
| **Actualización de Análisis de Riesgos de Continuidad del Servicio del Poder Judicial** |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Código | Fecha Elaboración | Fecha Actualización | Nº Revisión | Página |
| IFME-SGCS-DE-31-1988-008 | 06/12/2023  |  | 01 | 1  |



ACTUALIZACIÓN DE ANÁLISIS DE RIESGOS DE CONTINUIDAD DEL SERVICIO DEL PODER JUDICIAL

# **Control de Cambios**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Versión | Fecha | Realizado por | Motivo | Firma |
| 01  | 06/12/2023  | Subproceso de Gestión de la Continuidad del Servicio  | Final |   |
|  |  |  |  |   |
|  |  |  |  |   |
|  |  |  |  |   |

# **Control de Aprobación**

|  |  |  |  |
| --- | --- | --- | --- |
| Sello  | Elaboró  | Revisó  | Autorizó  |
|   | Subproceso de Gestión de la Continuidad del Servicio | Dirección Ejecutiva | Comité Técnico de Continuidad del Servicio  |
| Firma  | Firma  | Firma  |

Este documento es propiedad intelectual del Poder Judicial de la República de Costa Rica; y contiene información confidencial únicamente para uso interno de la Institución. Si usted no tiene permiso para este documento, debe devolverlo a la Dirección Ejecutiva y además, se le notifica que cualquier divulgación, copia, distribución o realizar cualquier acción basada en este documento está estrictamente prohibido.

**Contenido**

[**Control de Cambios** 2](#_Toc155778512)

[**Control de Aprobación** 2](#_Toc155778513)

[**1.**  **Introducción** 5](#_Toc155778514)

[**2.** **Objetivo y Alcance del Documento** 6](#_Toc155778515)

[**3.** **Antecedentes** 7](#_Toc155778516)

[**4.**  **Documentación de referencia** 8](#_Toc155778517)

[**5.**  **Definiciones** 8](#_Toc155778518)

[**6.** **Metodología** 11](#_Toc155778519)

[Tabla 1: Porcentaje asociada a la probabilidad de ocurrencia del riesgo. 12](#_Toc155778520)

[Tabla 2: Puntaje asociada al impacto del riesgo. 12](#_Toc155778521)

[Tabla 3: Estimación nivel de riesgo inherente. 13](#_Toc155778522)

[Tabla 4: Declaración del apetito de riesgo en el Poder Judicial. 13](#_Toc155778523)

[Tabla 5: Intervalo de categorización para el nivel de riesgo inherente. 14](#_Toc155778524)

[**7.**  **Identificación y análisis de riesgos** 14](#_Toc155778525)

[Tabla 6. Identificación de riesgos de continuidad en el Poder Judicial. 15](#_Toc155778526)

[Gráfico 1. Mapa gráfico de identificación de riesgos de continuidad en el Poder Judicial. 17](#_Toc155778527)

[7.1 Indisponibilidad tecnológica 17](#_Toc155778528)

[Tabla 7. Nivel de riesgo inherente para el escenario disruptivo de Indisponibilidad tecnológica. 18](#_Toc155778529)

[7.2 Indisponibilidad del recurso humano 19](#_Toc155778530)

[Tabla 8. Nivel de riesgo inherente para el escenario disruptivo de Indisponibilidad del recurso humano. 20](#_Toc155778531)

[7.3 Indisponibilidad de la infraestructura física 20](#_Toc155778532)

[Tabla 9. Nivel de riesgo inherente para el escenario disruptivo de Indisponibilidad de la infraestructura física. 21](#_Toc155778533)

[7.4 Dependencia de proveedores externos 21](#_Toc155778534)

[Tabla 10. Nivel de riesgo inherente para el escenario disruptivo de Dependencia de proveedores externos. 22](#_Toc155778535)

[7.5 Carencia de insumos para la prestación del servicio 23](#_Toc155778536)

[Tabla 11. Nivel de riesgo inherente para el escenario disruptivo de Carencia de insumos. 23](#_Toc155778537)

[Tabla 12. Mapa de calor de SEVRI para los escenarios de riesgo global de disrupción a la continuidad del servicio en el Poder Judicial. 24](#_Toc155778538)

[**8.** **Análisis de riesgos y gestión de la continuidad** 25](#_Toc155778539)

[Gráfico 2. Tendencia del impacto de riesgos de continuidad ante medidas de administración. 27](#_Toc155778540)

[Gráfico 3. Relación de modelos de gestión con la continuidad del servicio institucional. 28](#_Toc155778541)

[**9.**  **Tratamiento de riesgos de disrupción** 29](#_Toc155778542)

[Tabla 13. Ejemplo: Matriz de respuesta a riesgos de continuidad. 29](#_Toc155778543)

[**10.**  **Conclusiones** 34](#_Toc155778544)

[**11.**  **Recomendaciones** 37](#_Toc155778545)

# **1. Introducción**

Según la norma ISO 22301 *“Sistemas de gestión de la continuidad del negocio”*, la Continuidad del Servicio es un término utilizado para referirse a las estrategias y planificación mediante las cuales las organizaciones se preparan para continuar con la entrega de sus productos y servicios, dentro de plazos aceptables a una capacidad predefinida, durante un evento disruptivo generado por eventos catastróficos tales como incendios, inundaciones, ataques cibernéticos, accidentes, errores humanos, entre otros. En la misma línea, un Sistema de Gestión de Continuidad del Servicio (SGCS) ayuda a las organizaciones a prepararse para enfrentar esas emergencias, a gestionar las crisis y mejorar su capacidad de recuperación operacional, asegurar la continuidad de la gestión de las funciones dentro de la organización, contar con planes de trabajo a fin de evitar, prevenir o disminuir la afectación en la prestación de los servicios organizacionales catalogadas como críticos o esenciales; de manera que los esfuerzos se dirigen a mantener la continuidad de esos servicios ante eventos disruptivos, en beneficio de las personas usuarias.

En el caso del Poder Judicial de Costa Rica, en sesión del Consejo Superior número 48-2022, celebrada el 7 de junio de 2022, artículo LXXV (acuerdo confidencial), entre otros puntos, se avaló *la conformación del “Proceso de Gestión de Continuidad del Servicio”, como un nuevo proceso institucional, de naturaleza crítica y estratégica dentro del Poder Judicial*. Esto implica que a nivel de toda la organización, la continuidad del servicio se aborda con un tema de sumo interés; lo cual es concordante con la Ley General de Administración Pública, que en su artículo 4 establece la obligación de que todos los servicios públicos deben cumplir con principios y entre ellos está la continuidad del servicio; así como y el artículo 14 de la Ley General de Control Interno que establece el **deber** del jerarca y de los titulares subordinados de analizar y valorar los riesgos y adoptar las medidas necesarias para disminuir el nivel de riesgo, en este caso sobre la interrupción del servicio público que presta el Poder Judicial.

La Guía de Implementación de la norma ISO 22301:2019 indica que:

*“El propósito de la norma no es necesariamente lograr la mitigación total del impacto de la interrupción, sino de ayudar a una organización a comprender la magnitud y el tipo de impacto que está dispuesta a aceptar después de una interrupción para lo cual la organización desarrolla un sistema de continuidad del negocio dimensionado correctamente para sus necesidades”.* (El subrayado ha sido agregado).

Un Sistema de Gestión de Continuidad del Servicio (SGCS) es una agrupación de métodos, procedimientos y normas interrelacionados para salvaguardar la continuidad de los procesos y servicios críticos o esenciales. La norma orienta a que el establecimiento del sistema da la capacidad a la organización para controlar, evaluar y continuar mejorando la continuidad del servicio.

La gestión de los riesgos de continuidad es parte del sistema. Por ello, la norma INTE G130:2022/Cor 1:2023 *“Sistemas de Gestión de Continuidad de Servicios para organizaciones públicas y sin fines de lucro- Requisitos y orientación para su uso”* determina que la organización debe realizar la evaluación de riesgos a intervalos planificados y cuando haya cambios significativos dentro de la organización o el contexto en que opera.

Particularmente esta norma indica:

*“8.2.3 Evaluación de riesgos*

*La organización debe implementar y mantener un proceso de evaluación de riesgos.*

*La organización pública y sin fines de lucro debe:*

*a) identificar los riesgos de disrupción para las actividades priorizadas de la organización y de los recursos requeridos;*

*b) analizar y evaluar los riesgos identificados;*

*c) determinar cuáles riesgos requieren tratamiento”.*

La identificación y análisis de los riesgos de continuidad que enfrenta la institución debe contemplar tanto las fuentes internas como externas pertinentes para la consecución de los objetivos vinculados a la continuidad del servicio.

Los terremotos, tormentas, huelgas, pandemias, entre otros, son solo algunas de las amenazas a las que ha estado expuesto el Poder Judicial en los últimos años. Cuando ocurren, todas estas situaciones pueden causar la interrupción de las operaciones o servicios de la institución en diferentes áreas y niveles de impacto; y son las experiencias vividas las que han evidenciado estos riesgos y las consecuencias reales de su materialización.

Como parte del Plan General de Continuidad del Servicio, en 2016 el Poder Judicial desarrolló un análisis de riesgos de continuidad a nivel institucional, el cual ofreció una primera percepción de los riesgos potenciales que podrían ocasionar una interrupción de su operación. Posteriormente, en el año 2020 el Consejo Superior aprobó el *“Informe de Análisis de Riesgos de Continuidad del Servicio del Poder Judicial”*; sin embargo, desde entonces el contexto interno de la organización (por ejemplo, las personas, los procesos y la tecnología), así como su entorno externo (por ejemplo, el ambiental, político, social y económico) han cambiado, de forma que los riesgos identificados en su momento deben ser revisados a la luz de dichos cambios.

Por tanto, en este informe se aborda a identificación de riesgos, a la luz de los eventos disruptivos materializados o que pueden presentar mayor probabilidad de ocurrencia dentro del Poder Judicial.

# **2. Objetivo y Alcance del Documento**

El **objetivo general** abordado en este documento es:

Ponderar los riesgos de disrupción para las actividades priorizadas del Poder Judicial, de acuerdo con los recientes cambios en la organización y en el contexto.

**Objetivos específicos:**

* Identificar los riesgos de continuidad vinculados a los procesos y servicios institucionales, que resultan críticos o esenciales para el Poder Judicial.
* Categorizar los distintos tipos de riesgos de continuidad, según escenarios de disrupción que podrían afectar al Poder Judicial.

**El alcance** contempla la identificación y análisis de los riesgos de continuidad que enfrenta la institución y que debe examinar tanto de las fuentes internas como externas pertinentes, para la consecución de los objetivos vinculados a la continuidad del servicio. De manera que el enfoque de este informe aborda la identificación de riesgos, a la luz de los eventos disruptivos materializados o que presentan mayor probabilidad de ocurrencia dentro del Poder Judicial; considerando la categorización de los riesgos para su posterior tratamiento.

Los resultados de esta evaluación ayudarán al Poder Judicial a determinar las opciones de gestión de riesgo adecuadas, así como priorizar las medidas de protección y mitigación que formarán parte de la estrategia de continuidad del servicio institucional.

Se excluye del presente análisis la selección y descripción detallada de las medidas de tratamiento de los riesgos que superan el apetito de la institución para cada proceso o servicio crítico o esencial. Estas acciones de mitigación estarán detalladas en la estrategia de continuidad del servicio, que corresponde a otra etapa del Sistema de Gestión de Continuidad del Servicio.

# **3. Antecedentes**

El Consejo Superior en la sesión 103-2019 celebrada el 26 de noviembre de 2019, artículo XXIV, aprobó *el “Informe del Análisis de Impacto al Servicio del Poder Judicial”.* En dicho informe se reportó el resultado de la labor realizada para esa etapa, donde se identificaron un total de 688 procesos institucionales, de los cuales 64 se priorizaron como procesos que resultan críticos, en caso de ocurrir un evento disruptivo que afecte la continuidad normal de los servicios.

Posteriormente, en la sesión del Consejo Superior número 72-2020, celebrada el 16 de julio de 2020, artículo XIII, se conoció y aprobó el *“Informe de Análisis de Riesgos de Continuidad del Servicio del Poder Judicial”*, el cual fue elaborado con el trabajo de la organización consultora a la que se le adjudicó la Licitación Abreviada 2016LA-000063-PROV, denominada *“Contratación de horas de Asesoría Profesional para el Desarrollo de las Fases III, IV y V del Plan General de Continuidad de Servicio del Poder Judicial”.*

Se considera también el *“Informe del seguimiento del manejo de los riesgos de continuidad”* el cual tuvo como finalidad resaltar las estrategias del Poder Judicial durante la definición de su Plan General de Continuidad del Servicio que se pueden relacionar con escenarios de riesgo como el de la crisis generada por el COVID-19; además de contrastar las acciones realizadas por la institución durante esta contingencia con lo planificado, para determinar las fortalezas y las oportunidades de mejora a nivel de gestión y operativas cuando sea necesario en el futuro.

Por otra parte, se toma en cuenta para el presente informe la Circular 264-2023 de la Secretaría General de la Corte, referente al *“Portafolio y Estructura de Riesgos Institucional, versión 2023”* elaborado por la Oficina de Control Interno, donde se contemplan eventos que podrían atentar contra la consecución de los objetivos institucionales, incluidas las amenazas a la “Gestión del Servicio a las personas usuarias”, con el evento “Desmejoramiento del servicio proporcionado a las personas usuarias”.

# **4. Documentación de referencia**

* ISO 22301:2012 Business continuity management systems -- Requirements, International Organization for Standardization (ISO).
* ISO 31000:2011 Gestión del riesgo. Principios y directrices.
* Norma INTE G130:2022/Cor 1:2023 “Sistemas de Gestión de Continuidad de Servicios para organizaciones públicas y sin fines de lucro- Requisitos y orientación para su uso”.
* International Glossary of Resiliency, DRI International.
* Informe de Análisis de Riesgos de Continuidad del Servicio del Poder Judicial, aprobado por el Consejo Superior en la sesión 72-2020 celebrada el 16 de julio de 2020, artículo XIII.
* Política de Gestión de la Continuidad del Servicio, Poder Judicial. Versión aprobada por la Corte Plena en Sesión No. 37-14 de 4 de agosto del 2014, artículo XII.
* Instructivo para la elaboración del Sistema Específico de Valoración de Riesgo Institucional (SEVRI). Oficina de Control Interno del Poder Judicial, versión de mato 2022.
* Marco Metodológico del Análisis de Riesgos de Continuidad del Servicio. Subproceso de Gestión de Continuidad del Servicio, versión 2023.

# **5. Definiciones**

| **Palabra/Término** | **Definición** |
| --- | --- |
| Amenaza  | Situación o condición natural u ocasionada por el hombre que puede causar una interrupción de las operaciones o servicios de una organización. Tomado de International Glossary of Resiliency (Glosario en español), DRI International.  |
| Amenazas ocasionadas por el ser humano | Causas de una posible interrupción en las operaciones como resultado de acciones realizadas por el ser humano identificadas en la evaluación de riesgos, por ejemplo, personal inconforme, terrorismo, chantaje, protestas laborales, huelgas, disturbios sociales, etc. Tomado de International Glossary of Resiliency (Glosario en español), DRI International. |
| Análisis de Impacto al Negocio o Servicio (BIA o SIA, por sus siglas en inglés)  | Proceso de evaluación de las operaciones y del efecto que una interrupción tendría en ellas. Incluye no sólo el análisis de impacto al negocio o servicio, que es la identificación de los activos, funciones, procesos y recursos críticos, sino también la evaluación de los posibles daños o pérdidas que pudieran afectar a la organización como resultado de una interrupción o un cambio en el negocio. Tomado de International Glossary of Resiliency (Glosario en español), DRI International.  |
| Análisis de riesgos  | Proceso de cuantificación de las amenazas a una organización y la probabilidad de que se materialicen. Tomado de International Glossary of Resiliency (Glosario en español), DRI International.  |
| Apetito de riesgo  | El apetito es el nivel de riesgo que la organización está dispuesta a aceptar, tolerar o estar expuesta en cualquier punto en el tiempo. Su tolerancia será la desviación respecto a ese nivel de riesgo. La capacidad será el nivel máximo de riesgo que una organización puede soportar en la consecución de sus objetivos. Tomado de International Glossary of Resiliency (Glosario en español), DRI International.  |
| Continuidad del servicio | Capacidad de una organización para continuar con la entrega de sus productos y servicios dentro de plazos aceptables a una capacidad predefinida durante un evento disruptivo.Tomado de INTE G130:2022/Cor 1:2023 “Sistemas de Gestión de Continuidad de Servicios para organizaciones públicas y sin fines de lucro- Requisitos y orientación para su uso”. |
| Control  | Medios de gestión de riesgos, como políticas, procedimientos, directrices, prácticas o estructuras organizacionales, que pueden ser de carácter administrativo, técnico, de gestión o legal. Tomado de International Glossary of Resiliency (Glosario en español), DRI International. |
| Estrategia de continuidad del negocio  | Curso de acción definido previamente (y aprobado por el órgano directivo) con el fin de proteger la viabilidad de la organización y reanudar sus actividades críticas en los plazos establecidos. Las estrategias seleccionadas deben cubrir los RTO identificados en el BIA. Tomado de International Glossary of Resiliency (Glosario en español), DRI International.  |
| Impacto  | Efecto, aceptable o no, que un evento tiene en una organización. Los tipos de impactos al negocio son normalmente descritos como financieros y no financieros, y posteriormente se dividen en tipos específicos, dependiendo del sector. Tomado de International Glossary of Resiliency (Glosario en español), DRI International.  |
| Interrupción  | Evento que detiene las funciones, operaciones o procedimientos habituales de la organización, sea este previsto (por ejemplo, huracanes, disturbios políticos) o imprevistos (por ejemplo, un apagón eléctrico, un ataque terrorista o una falla de la tecnología). Tomado de International Glossary of Resiliency (Glosario en español), DRI International. |
| Pandemia  | Enfermedad epidémica o infecciosa que puede tener un impacto a nivel mundial. Tomado de International Glossary of Resiliency (Glosario en español), DRI International.  |
| Servicio crítico o esencialen el Poder Judicial | *“Son aquellos relacionados con actividades de la institución que están sujetos al cumplimiento de plazos u obligaciones legales, la protección de derechos fundamentales, o cuya suspensión puede ocasionar un perjuicio a la vida de las personas, una afectación grave a la operación interna, o provocar una pérdida de recursos o activos institucionales y una degradación de la imagen institucional”.*Subproceso de Gestión de la Continuidad del Servicio del Poder Judicial, adaptación de definición aportada por la Contraloría General de la República en la Resolución R-DC-006-2021 “Directrices de continuidad para la generación de valor público en la CGR”. |
| Probabilidad  | Posibilidad verosímil y fundada de que algo suceda, haya sido esto definido, medido o estimado objetiva o subjetivamente. Tomado de International Glossary of Resiliency (Glosario en español), DRI International.  |
| Riesgo  | Probabilidad de que se presente un evento que pudiera causar daños o pérdidas o afectar la capacidad para alcanzar los objetivos del negocio, asociado a la vulnerabilidad de la organización ante esa amenaza. Tomado de International Glossary of Resiliency (Glosario en español), DRI International. También se le describe como la *“Probabilidad de que un factor, acontecimiento o acción, sea de origen interno o externo, afecte de manera adversa a la organización, área, proyecto o programa y perjudique el logro de sus objetivos.”*Tomado del glosario de términos de la Oficina de Control Interno del Poder Judicial (<https://controlinterno.poder-judicial.go.cr/index.php/glosario-de-terminos>). |
| Riesgo inherente | Es aquel nivel de riesgo que NO toma en cuenta la aplicación de los controles al momento de valorar el parámetro de probabilidad de ocurrencia.Oficina de Control Interno del Poder Judicial, Instructivo para la elaboración del Sistema Específico de Valoración de Riesgo Institucional (SEVRI), versión 2022.  |
| Riesgo residual  | Nivel de riesgo remanente después de que se han implementado todas las acciones costo-efectivas para reducir el impacto, la probabilidad y las consecuencias de un riesgo o grupo de riesgos específicos, sujeto al apetito al riesgo de una organización. Tomado de International Glossary of Resiliency (Glosario en español), DRI International.  |
| Prevención del riesgo | Estrategia de administración del riesgo que se utiliza cuando se pueden aplicar acciones anticipadas sobre las **fuentes de un riesgo**, para disminuir su probabilidad de ocurrencia o impacto.Oficina de Control Interno del Poder Judicial, Estrategias de respuesta al riesgo. |
| Mitigación del riesgo | Estrategia de administración del riesgo que comprende las acciones que se planifican antes de que ocurra un riesgo, de tal manera que, en caso de suceder una emergencia, se activen para reducir **su impacto** a niveles tolerables y costo razonable. Oficina de Control Interno del Poder Judicial, Estrategias de respuesta al riesgo. |
| Fuente de riesgo | Elemento que solo o en combinación, tiene el potencial intrínseco para generar un riesgo.ISO 31000 Risk management — Principles and guidelines. First edition 2009-11-15. |

# **6. Metodología**

El análisis de riesgo del presente informe parte del *“Análisis de Riesgos de Continuidad del Servicio del Poder Judicial”,* aprobado por el Consejo Superior en la sesión 72-2020 celebrada el 16 de julio de 2020, artículo XIII; y toma como guía el Marco Metodológico del Análisis de Riesgos de Continuidad del Servicio en su versión 2023, elaborado por el Subproceso de Gestión de Continuidad del Servicio.

En la primera etapa de este nuevo análisis se cuantificó la recurrencia de cada factor o fuente de riesgo identificado por los dueños de procesos y servicios críticos, posteriormente se clasificó la frecuencia en una matriz que se categorizó según cinco tipos de escenarios de riesgo que se identificaron.

De acuerdo con la categorización y la participación relativa de cada factor o fuente de riesgo de disrupción, se aplicó un análisis donde se utilizó la metodología del SEVRI, que es guiado por la Oficina de Control Interno del Poder Judicial. Según dicha metodología, se considera la probabilidad de ocurrencia de los factores y su posible impacto, con los siguientes parámetros, para determinar el riesgo global:

#### Evaluación de probabilidad

Se considera la probabilidad de que las amenazas identificadas se presenten en el Poder Judicial. Para ello se toma en cuenta la frecuencia (o recurrencia) con la que los factores fueron identificados y las experiencias vividas de su materialización; así como la cantidad de los procesos o servicios a los cuales podría afectar, que se valora a nivel global (institucional).

En la tabla 1 se muestran los criterios para la evaluación de la probabilidad definidos en el SEVRI-PJ.

## Tabla 1: Porcentaje asociada a la probabilidad de ocurrencia del riesgo.

|  |  |
| --- | --- |
| **Probabilidad de ocurrencia** | **Porcentaje** |
| Muy probable | 90 |
| Bastante probable | 70 |
| Probable | 50 |
| Poco probable | 30 |
| Improbable | 10 |

Fuente: SEVRI-PJ.

#### Evaluación del impacto

Al contar con las categorías de riesgos de disrupción identificados y sus diferentes factores, se considera la magnitud del impacto a nivel global (en consecuencia, en la institución), tomando en cuenta la experiencia acumulada y los procesos o servicios a los cuales afecta cada caso.

La tabla 2 muestra los criterios para la evaluación del impacto utilizados, los cuales se encuentran definidos en el SEVRI-PJ.

## Tabla 2: Puntaje asociada al impacto del riesgo.

|  |  |
| --- | --- |
| **Impacto** | **Puntaje** |
| Muy alto | 5 |
| Alto | 4 |
| Moderado | 3 |
| Bajo | 2 |
| Muy bajo | 1 |

Fuente: SEVRI-PJ.

#### Estimación del nivel de riesgo inherente

A partir de la evaluación del impacto de las amenazas de continuidad del servicio y de su probabilidad de ocurrencia, se realizó la estimación del nivel de riesgo inherente para cada una de las categorías de riesgo evaluadas. El cálculo del riesgo estimado se realizó multiplicando el valor del impacto por el valor de la probabilidad.

|  |
| --- |
| **Riesgo = Probabilidad de ocurrencia x Impacto**  |

La Tabla 3 muestra el valor de riesgo resultante para cada nivel de impacto y probabilidad definidos en el SEVRI-PJ.

## Tabla 3: Estimación nivel de riesgo inherente.

| **Escenario de riesgo** | **Probabilidad de ocurrencia (PO)** | **Impacto****(I)** | **Nivel de riesgo inherente** | **Justificación (Probabilidad e Impacto)** |
| --- | --- | --- | --- | --- |
| **Se cita el riesgo** | Puntaje según categorías | Puntaje según categorías | Producto obtenido de (PO x I) | Clasificación de la categoría según el puntaje obtenido | **PO:** Se anota la justificación del valor de probabilidad asignada.**I:** Se anota la justificación del valor de impacto asignado.  |

Fuente: SEVRI-PJ.

**Valoración de riesgos**

Con base en los resultados de la fase de análisis, se realiza la valoración de riesgos al comparar el registro de las categorías de riesgos de continuidad contra la declaración del apetito de riesgo o nivel de riesgo aceptable (NRA).

El apetito es el nivel de riesgo que el Poder Judicial está dispuesto a aceptar o tolerar en cualquier punto en el tiempo, por lo que cualquier riesgo que supere ese nivel debería ser administrado a fin de reducir su impacto o probabilidad de ocurrencia, al punto de que el nuevo nivel de riesgo pueda ser aceptado.

## Tabla 4: Declaración del apetito de riesgo en el Poder Judicial.

|  |  |  |
| --- | --- | --- |
|   |   | **Impacto** |
|   |   | **Muy bajo1** | **Bajo2** | **Moderado3** | **Alto4** | **Muy alto5** |
| **Probabilidad** | **Muy probable90** | **90** | **180** | **270** | **360** | **450** |
| **Bastante probable70** | **70** | **140** | **210** | **280** | **350** |
| **Probable50** | **50** | **100** | **150** | **200** | **250** |
| **Poco probable30** | **30** | **60** | **90** | **120** | **150** |
| **Improbable10** | **10** | **20** | **30** | **40** | **50** |

Fuente: SEVRI-PJ.

De acuerdo con lo establecido en el SEVRI-PJ, el apetito de riesgo definido por el Poder Judicial serán aquellos riesgos ubicados en los niveles “Muy bajo” y “Bajo”, tal como se muestra en la Tabla 5. Estos riesgos podrían ser aceptados por la institución sin necesidad de implementar controles adicionales, aunque se deben monitorear igualmente ante los cambios en el contexto externo e interno que puedan requerir la revisión del análisis realizado.

## Tabla 5: Intervalo de categorización para el nivel de riesgo inherente.

|  |  |
| --- | --- |
| **Intervalo** | **Nivel de Riesgo Inherente** |
| 0 < X <= 119 | Bajo / Muy bajo |
| 120 <= X <= 249 | Medio |
| 250 <= X <= 450 | Alto |

Fuente: SEVRI-PJ.

La importancia de esta etapa es que permite comprender el riesgo obtenido mediante el análisis y ayuda a la toma de decisiones, proporcionando contexto sobre cuáles son los riesgos que superan el criterio de aceptación de la institución y se deben administrar, según su respectiva prioridad. Con este conocimiento se pueden establecer los planes y estrategias para salvaguardar la vida de las personas y mitigar los impactos de un evento disruptivo en los procesos o servicios críticos del Poder Judicial.

# **7. Identificación y análisis de riesgos**

En el análisis de riesgos realizado en el año 2020 por el personal de los despachos y oficinas dueñas de procesos críticos se identificaron los diferentes factores o fuentes de riesgo que podrían impedir la continuidad de los servicios; esto es: riesgos de disrupción, tomando en cuenta que, según lo cita la Norma INTE G130:2022, *“El riesgo a menudo se caracteriza por la referencia a potenciales eventos y consecuencias"* o como lo indica la normativa de control interno, la *“probabilidad de que ocurran eventos de origen interno o externo, que tendrían consecuencias sobre el cumplimiento de los objetivos institucionales o de la oficina en particular”.*

La identificación correspondiente se retomó en este informe con la cuantificación de la recurrencia de cada factor o fuente al momento de ser citado por las personas expertas según cada proceso o servicio. Posteriormente, los factores de disrupción se categorizaron en escenarios de riesgo según el origen o consecuencia; de lo cual han salido a la luz cinco tipos: **a)** riesgos asociados a “Indisponibilidad del recurso humano”, **b)** riesgos asociados a la “Indisponibilidad de la infraestructura física”; **c)** riesgos vinculados a la “Indisponibilidad tecnológica”; **d)** riesgos de continuidad derivados de “Dependencia de proveedores externos” y **e)** riesgos de continuidad por “Carencia de insumos”.

El resultado de la cuantificación se muestra en la siguiente tabla, donde se presenta la frecuencia o recurrencia; esto es, la cantidad de veces que el riesgo de disrupción fue identificado y citado; además se presenta su distribución porcentual con respecto al total general y se ha resaltado en color los riesgos para los cuales se tiene conocimiento de su materialización.

## Tabla 6. Identificación de riesgos de continuidad en el Poder Judicial.

| **Factores de riesgo / Escenarios de riesgo** | **Frecuencia** | **Distribución porcentual** |
| --- | --- | --- |
|   |   |   |
| **Indisponibilidad del recurso humano** |  |  |
| Enfermedades por plagas (zancudos, ratas, murciélagos, cucarachas, etc.).  | 3 | 0,6% |
| Retraso en el traslado del personal. | 3 | 0,6% |
| Obstrucción de vías o vías inhabilitadas.  | 4 | 0,8% |
| Indisponibilidad del personal informático. | 7 | 1,3% |
| Falta de personal capacitado o especializado. | 10 | 1,9% |
| Indisponibilidad o carencia del personal. | 47 | **8,9%** |
| **Subtotal del escenario** | **74** | **14,0%** |
|   |   |   |
| **Indisponibilidad de la infraestructura física** |  |  |
| Instalaciones inadecuadas para necesidades específicas. | 3 | 0,6% |
| Indisponibilidad de acceso físico. | 5 | 0,9% |
| Motines o vandalismo. | 6 | 1,1% |
| Indisponibilidad de las instalaciones. | 7 | 1,3% |
| Desastres industriales o en el espacio de trabajo. | 40 | **7,5%** |
| Fuego. | 42 | **7,9%** |
| Ataque externo (terrorismo, explosivos, secuestro). | 43 | **8,1%** |
| Desastres naturales. | 44 | **8,3%** |
| Daños por agua. | 45 | **8,5%** |
| **Subtotal del escenario** | **235** | **44,3%** |
|   |   |   |
| **Indisponibilidad tecnológica** |  |  |
| Falta de permisos de acceso a sistemas | 1 | 0,2% |
| Desactualización de sistemas o bases de datos. | 4 | 0,8% |
| Sobrecarga eléctrica. | 4 | 0,8% |
| Indisponibilidad de los sistemas de información. | 5 | 0,9% |
| Falla de sistemas o plataformas de operación | 6 | 1,1% |
| Falla de servicios de comunicaciones | 28 | **5,3%** |
| Acceso no autorizado a la infraestructura tecnológica y de comunicación que soporta el proceso.  | 36 | **6,8%** |
| Amenazas tecnológicas (destrucción de la información, averías de origen físico o lógico, caída del sistema por agotamiento de recursos, degradación de los soportes de almacenamiento de información, errores de mantenimiento, errores de configuración, manipulación de la configuración, abuso de privilegios de acceso, denegación de servicio, vulnerabilidades de los programas).  | 40 | **7,5%** |
| Corte del suministro eléctrico. | 43 | **8,1%** |
| **Subtotal del escenario** | **167** | **31,5%** |
|   |   |   |
| **Dependencia de proveedores externos** |  |  |
| Falta de seguridad externa o interna. | 1 | 0,2% |
| Ruptura de las relaciones con la agencia de Administración para el Control de Drogas (DEA). | 1 | 0,2% |
| Incumplimiento del proveedor especialista para realizar reparaciones.  | 2 | 0,4% |
| Indisponibilidad del proveedor del servicio | 3 | 0,6% |
| Indisponibilidad del proveedor de los sistemas de la DTIC.  | 3 | 0,6% |
| Interrupción de servicios públicos básicos. | 3 | 0,6% |
| Falta de combustible | 4 | 0,8% |
| Incumplimiento del proveedor de hospedaje CODISA.  | 4 | 0,8% |
| **Subtotal del escenario** | **21** | **4,0%** |
|   |   |   |
| **Carencia de insumos** |  |  |
| Falta de reactivos, estándares, otros insumos.  | 1 | 0,2% |
| Falta de repuestos | 1 | 0,2% |
| Indisponibilidad de insumos | 1 | 0,2% |
| Robo de equipos. | 1 | 0,2% |
| Unidades insuficientes (vehículos). | 2 | 0,4% |
| Carencia de equipo adecuado y necesario. | 4 | 0,8% |
| Falta de presupuesto.  | 4 | 0,8% |
| Indisponibilidad de la información | 4 | 0,8% |
| Falla de equipos base o soporte (aires acondicionados, alarmas, control de acceso). | 5 | 0,9% |
| Indisponibilidad de vehículos o transporte. | 10 | 1,9% |
| **Subtotal del escenario** | **33** | **6,2%** |
|   |   |   |
| **Totales de factores contabilizados** | **530** | **100%** |

**Fuente:** Elaboración propia a partir del “Informe de Análisis de Riesgos de Continuidad del Servicio del Poder Judicial”, 2020.

En la siguiente gráfica se muestra la distribución de los riesgos según su frecuencia de identificación, donde se debe tener en cuenta que, a mayor frecuencia, mayor probabilidad de ocurrencia y, en consecuencia, representan una mayor amenaza para el Poder Judicial.

## Gráfico 1. Mapa gráfico de identificación de riesgos de continuidad en el Poder Judicial.



**Fuente:** Elaboración propia a partir del estudio del “Informe de Análisis de Riesgos de Continuidad del Servicio del Poder Judicial”, 2020.

## 7.1 Indisponibilidad tecnológica

El gráfico permite visualizar que en el escenario de Indisponibilidad de la Tecnología existen varias fuentes o factores de riesgo identificados con mucha frecuencia. El corte de suministro eléctrico es el más recurrente por haberse identificado más veces, pero a la vez es un factor que se ha materializo para despachos y oficinas, principalmente en zonas periféricas donde no se cuenta con contingencia eléctrica (generadores eléctricos y UPS). La falla de servicios de comunicaciones (red institucional) es otro factor materializado que ha interrumpido la prestación de servicios, lo cual se une con la falla de sistemas o plataformas de operación, que se da en casos de equipos que dan soporte a centros de datos, tal como los sistemas de aire acondicionado, sin los cuales los centros de datos no pueden operar, ya que se expone a los equipos servidores a daños severos. El resultado es la indisponibilidad de la plataforma de tecnología.

Igualmente, el gráfico permite observar el riesgo latente de las amenazas tecnológicas y el acceso no autorizado a la infraestructura tecnológica. En particular, las amenazas tecnológicas tienen una variedad amplia de fuentes; entre ellos los riesgos de destrucción de la información, averías de origen físico o lógico, caída del sistema por agotamiento de recursos, degradación de los soportes de almacenamiento de información, errores de mantenimiento, errores de configuración, manipulación de la configuración, abuso de privilegios de acceso, denegación de servicio, vulnerabilidades de los programas. Todos ellos de gran sensibilidad para los servicios institucionales.

Esta condición de riesgo inherente pone de manifiesto la necesidad del Poder Judicial para implementar estrategias y acciones de continuidad, desde la prevención, en relación con los riesgos que pueden indisponer la plataforma tecnológica de la cual dependen los despachos y oficinas judiciales para la prestación de sus servicios; lo cual se evidencia en que, del total de factores de riesgo mapeados, el 31,5% corresponden a esta categoría tecnológica.

La siguiente tabla da cuenta del nivel de riesgo inherente de la indisponibilidad tecnológica, considerando la evidencia extraída de la identificación de riesgos de las personas dueñas de los procesos y servicios críticos institucionales.

## Tabla 7. Nivel de riesgo inherente para el escenario disruptivo de Indisponibilidad tecnológica.

| **Escenario de riesgo** | **Probabilidad de ocurrencia** | **Impacto** | **Nivel de riesgo inherente** | **Justificación (Probabilidad e Impacto)** |
| --- | --- | --- | --- | --- |
| **Indisponibilidad tecnológica** | Muy probable(90) | Muy alto(5) | **450** | **Alto** | **PO:** Este escenario se cataloga como muy probable pues se ha materializado y las causas pueden provenir de diferentes fuentes; desde cortes de energía eléctrica a fallas de recursos soporte en los centros de datos, fallas en sistemas o equipos de comunicación y amenazas potenciales como ciberataques. Su ocurrencia obliga al Poder Judicial a mantener vigilancia constante para proteger esta infraestructura.**I:** El impacto es muy alto pues el Poder Judicial tiene una gran cantidad de servicios que dependen de la plataforma tecnológica, entre lo cual se destaca la digitalización de servicios y en particular de los expedientes electrónicos.  |

**Fuente:** Elaboración propia a partir de metodología SEVRI-PJ, según datos recabados de análisis de riesgos para procesos y servicios críticos institucionales.

## 7.2 Indisponibilidad del recurso humano

Evidencia de lo sensible que es el capital humano en el Poder Judicial se tiene al observar que el 14% del total de la frecuencia de factores identificados están abarcados por el escenario de Indisponibilidad del recurso humano. Particularmente, la “indisponibilidad o carencia del personal” es el riesgo de mayor peso en este escenario, con un 8,9% del total de factores de disrupción identificados.

Adicionalmente, es necesario indicar que la indisponibilidad del recurso humano es un escenario que ya se ha materializado en el Poder Judicial, muy particular en el contexto de la pandemia originada por el COVID en el año 2020; pero también se ha presentado en otros sucesos de continuidad operativa de las oficinas o despachos donde se pueden presentar ausencias por incapacidades, huelgas (como la vivida a lo interno de la institución en el año 2018), medidas sanitarias por enfermedad, entre otros casos.

En esta misma categoría, la gráfica 1 resalta a la vista dos factores relevantes: capacitación y especialización del personal, junto con la indisponibilidad del personal informático.

Existen procesos y servicios críticos que están en manos de personas con formación especializada y, por tanto, su ausencia representaría una baja sumamente sensible para la continuidad de los servicios implicados. Este es el caso de personal técnico y operativo presente en el proceso de “Seguridad humana y física Poder Judicial”, personal del OIJ para atención de eventos de crisis (Atención de sitios de suceso) así como el personal encargado de la plataforma de comunicaciones radiales del OIJ o peritaje forense, personal especializado para autopsias en Patología Forense, también medicina legal e identificación de personas.

De manera similar, el personal informático vinculado a procesos o servicios críticos, así como aquellos responsables de la continuidad operativa de los sistemas informáticos y la plataforma tecnológica en general, también se constituye en personal clave para la continuidad de los servicios institucionales; lo cual es coherente con el escenario de indisponibilidad de los servicios tecnológicos. Además, este personal, por sus funciones, también cuenta con formación especializada que le lleva a una condición de dificultad para ser sustituido en caso de bajas, lo cual incide en la sensibilidad de este riesgo.

Lo indicado en estos últimos párrafos es un aspecto sumamente relevante, no por la recurrencia evidenciada de estos factores sino porque se vinculan a procesos o servicios críticos que requieren de personal con formación particular y, por tanto, ante su ausencia, el reemplazo puede ser difícil o imposible.

Finalmente, de manera particular es importante destacar que personal de despachos judiciales, por su materia o conocimiento especializado, también se puede catalogar como bajas sensibles para los procesos o servicios críticos que atienden. No obstante, ello dependerá de la medida en la que su reemplazo sea difícil.

En la tabla 8 se muestra el nivel de riesgo inherente pera este escenario, el cual se calcula con base en los diferentes aspectos expuestos.

## Tabla 8. Nivel de riesgo inherente para el escenario disruptivo de Indisponibilidad del recurso humano.

| **Escenario de riesgo** | **Probabilidad de ocurrencia** | **Impacto** | **Nivel de riesgo inherente** | **Justificación (Probabilidad e Impacto)** |
| --- | --- | --- | --- | --- |
| **Indisponibilidad del recurso humano** | Muy probable(90) | Muy alto(5) | **450** | **Alto** | **PO:** El riesgo se ha materializado a todo nivel institucional en diferentes momentos, tal como la pandemia del COVID-19, la huelga del personal judicial en el año 2018 y en otras situaciones, tal como incapacidades del personal.**I:** El impacto es muy alto pues los procesos y servicios del Poder Judicial dependen del recurso humano. El impacto es más severo en los casos donde los procesos o servicios dependen de personal especializado, tal como personal informático, peritos, médicos legales o forenses, especialistas en diferentes ámbitos; e incluso personal especialmente capacitado para cierto tipo de funciones.  |

**Fuente:** Elaboración propia a partir de metodología SEVRI-PJ, según datos recabados de análisis de riesgos para procesos y servicios críticos institucionales.

Se concluye que este escenario es de alto riesgo para el Poder Judicial ya que el recurso humano es componente fundamental en toda la operativa de la institución, en todos sus Ámbitos.

## 7.3 Indisponibilidad de la infraestructura física

La prestación de servicios institucionales depende del espacio físico donde se interacciona con las personas usuarias y se da el servicio cara a cara; de igual manera, la prestación del servicio sigue ligada a la presencialidad de las personas servidoras y funcionarias judiciales; de manera que este es un activo crucial en la gestión de la continuidad, ya sea porque se requiera de espacios físicos con condiciones especiales (salas de juicio y de audiencias, laboratorios, equipos) o porque el espacio corresponde al lugar mismo donde reside el mobiliario y equipo institucional, lo cual incluye toda la infraestructura física, tangible de la plataforma tecnológica.

El análisis de riesgos de disrupción muestra que el 44,3% del total de factores mapeados está ligado a la indisponibilidad de la infraestructura física. La figura 1 resalta a la vista que los daños por agua y los desastres naturales encabezan la lista, no solo por la recurrencia registrada, sino por haberse materializado en diferentes ocasiones a lo interno del Poder Judicial y por ser un factor externo al cual la institución está expuesta, según la realidad de nuestro país y las amenazas naturales. También, es pertinente indicar que, de los cinco escenarios de disrupción mapeados, el asociado a la infraestructura es el de mayor ponderación en su participación relativa.

El análisis de factores de riesgo también muestra que los desastres industriales o en el espacio de trabajo, el fuego y los ataques externos (atentados, vandalismo, amenazas de bomba, etc.) son latentes, con un alto potencial de materializarse y que, de presentarse, coartan la capacidad del poder judicial para la continuidad de los servicios.

## Tabla 9. Nivel de riesgo inherente para el escenario disruptivo de Indisponibilidad de la infraestructura física.

| **Escenario de riesgo** | **Probabilidad de ocurrencia** | **Impacto** | **Nivel de riesgo inherente** | **Justificación (Probabilidad e Impacto)** |
| --- | --- | --- | --- | --- |
| **Indisponibilidad de la infraestructura física** | Bastante probable(70) | Alto(4) | **280** | **Alto** | **PO:** Este escenario se ha materializado en algunos casos y ciertas zonas están más expuestas que otras por riesgos de desastres naturales o condiciones propias de la infraestructura donde residen los despachos y oficinas. Esto marca diferencias a nivel de todos los despachos y oficinas judiciales.**I:** El impacto es alto ya que la infraestructura física y los espacios de trabajo son requeridos para la prestación de los servicios judiciales, siendo que en algunos casos el espacio es especializado para la labor, tal como celdas, salas de audiencias y salas de juicio, laboratorios, espacios médicos especialmente acondicionados, como ocurre con Patología Forense.  |

**Fuente:** Elaboración propia a partir de metodología SEVRI-PJ, según datos recabados de análisis de riesgos para procesos y servicios críticos institucionales.

## 7.4 Dependencia de proveedores externos

Existen procesos y servicios críticos que tienen dependencia de proveedores externos. Es el caso de ciertos servicios tecnológicos contratados a proveedores para albergar equipos y centros de datos, así como la provisión de servicios de soporte y otros equipos o recursos que son suministrados por terceros al Poder Judicial. También los servicios de seguridad dependen de este factor y el mantenimiento de equipos, tales como respaldos de energía eléctrica (UPS) o de equipos de aires acondicionados (muy sensibles para los centros de datos). Se incluyen en estos casos el suministro de combustible y los servicios básicos suministrados por organizaciones públicas, junto con servicios de enlaces de comunicaciones donde también pueden participar organizaciones privadas. En esta categoría se contempla también la provisión del información o servicios de proveedores, tal como la plataforma del Sistema de Depósitos Judiciales (SDJ) que provee el Banco de Costa Rica, o servicios del Registro Nacional, entre otras instituciones públicas, incluida la plataforma del Sistema Institucional de Compras Públicas (SICOP).

La falla o incumplimiento de estos proveedores externos pueden ser una fuente de riesgo para el escenario que pone sobre la mesa el riesgo de estas dependencias. En ese sentido, la tabla 10 muestra el nivel de riesgo asociado a este escenario.

## Tabla 10. Nivel de riesgo inherente para el escenario disruptivo de Dependencia de proveedores externos.

| **Escenario de riesgo** | **Probabilidad de ocurrencia** | **Impacto** | **Nivel de riesgo inherente** | **Justificación (Probabilidad e Impacto)** |
| --- | --- | --- | --- | --- |
| **Dependencia de proveedores externos** | Probable(50) | Alto(4) | **200** | **Medio** | **PO:** Este escenario es probable ya que se ha materializado en servicios del Poder Judicial que requieren de proveedores externos para suministrarle información, bienes y servicios. En diferentes aspectos el Poder Judicial depende de estos aliados para contar con recursos que permiten a la institución mantener su provisión de servicios. **I:** El impacto es muy alto ya que el Poder Judicial requiere contar con los bienes o servicios de proveedores para su propio funcionamiento. Ejemplo de ello son la plataforma del SDJ del Banco de Costa Rica, suministro de combustible, información de instituciones como el Ministerio de Justicia, servicios del Registro Nacional y otros proveedores como el INS, CODISA, ICE, organizaciones de seguridad, entre otras.  |

**Fuente:** Elaboración propia a partir de metodología SEVRI-PJ, según datos recabados de análisis de riesgos para procesos y servicios críticos institucionales.

## 7.5 Carencia de insumos para la prestación del servicio

Existen procesos o servicios que dependen de insumos particulares para garantizar la continuidad del servicio.

Los laboratorios de Medicina Legal y Medicina Forense son particularmente sensibles a este factor. Igualmente, la flotilla institucional que depende de repuestos y mantenimientos de los vehículos, que a su vez son necesarios para la prestación de servicios de transporte del OIJ o administrativo, así como la Oficinas de Comunicaciones Judiciales que también requieren de vehículos de transporte para su labor. En estas áreas resalta la carencia de equipo adecuado y necesario para la labor de las oficinas, lo que hace que este escenario se perfile como particular para oficinas del Ámbito Auxiliar de Justicia y el Administrativo.

Por otra parte, la gráfica 1 revela que la falla de equipos base o soporte es sumamente relevante a todo nivel institucional; estos son, por ejemplo, equipos de aire acondicionado en centros de datos, pues ante su fallo se deben apagar los equipos servidores (este es un riesgo que ya se ha materializado en circuitos judiciales); igualmente sucede con otros equipos como UPS o plantas de generación eléctrica. Estos factores son riesgos por sí mismos para la continuidad del servicio, pero a la vez fuente de riesgo para otros escenarios, tal como el de indisponibilidad de la plataforma tecnológica, por existir una dependencia en los recursos.

Debido a lo indicado, la “Carencia de insumos” se clasifica con un nivel de riesgo inherente medio, tal como se muestra en la tabla 11.

## Tabla 11. Nivel de riesgo inherente para el escenario disruptivo de Carencia de insumos.

| **Escenario de riesgo** | **Probabilidad de ocurrencia** | **Impacto** | **Nivel de riesgo inherente** | **Justificación (Probabilidad e Impacto)** |
| --- | --- | --- | --- | --- |
| **Carencia de insumos** | Probable(50) | Alto(4) | **200** | **Medio** | **PO:** Este escenario es probable pues se ha materializado en algunos casos o se han presentado situaciones de amenaza de su materialización; por ejemplo, con carencia de insumos en Ciencias Forenses. Se han presentado casos de falla de equipos de soporte como los aires acondicionados o UPS para centros de datos que han generado incidentes tecnológicos y como consecuencia, la interrupción de servicios.**I:** El impacto es categorizado como alto debido a que los factores de riesgo agrupados en este escenario afectan a procesos y servicios críticos del Poder Judicial, donde la dependencia de los insumos o equipos de soporte es alta.  |

**Fuente:** Elaboración propia a partir de metodología SEVRI-PJ, según datos recabados de análisis de riesgos para procesos y servicios críticos institucionales.

Finalmente, a modo de resumen, la tabla 12 muestra el mapa de calor del SEVRI para los riesgos inherentes valorados en las tablas anteriores. Tal como se puede observar en dicha tabla, conforme con el apetito de riesgo institucional, los cinco escenarios de riesgos de disrupción identificados se catalogan en las zonas roja y amarilla; es decir, **riesgo Alto y Medio**; lo cual implica que a nivel institucional se deben establecer controles para evitar, transferir, prevenir o mitigar el impacto de estos riesgos.

## Tabla 12. Mapa de calor de SEVRI para los escenarios de riesgo global de disrupción a la continuidad del servicio en el Poder Judicial.



**Fuente:** Elaboración propia a partir de metodología SEVRI-PJ, según datos recabados de análisis de riesgos para procesos y servicios críticos institucionales.

# **8. Análisis de riesgos y gestión de la continuidad**

En la gestión de la continuidad existen etapas clave: dos de las primeras (en orden de construcción) son la identificación de los procesos y servicios críticos que se realiza en el Análisis de Impacto al Servicio y posteriormente, la identificación de riesgos de disrupción asociada a los procesos y servicios críticos.

En el análisis de riesgos se identifica y se documentan aquellos eventos o amenazas que podrían impactar la continuidad del servicio de los procesos críticos del Poder Judicial y así, provocar una pérdida potencial para la institución. Su importancia reside en el hecho de que la institución solo podrá controlar eficazmente los eventos disruptivos que conoce y ha evaluado consistentemente.

Según el apetito al riesgo, la institución podría aceptar aquellos riesgos ubicados en los niveles “Muy bajo” y “Bajo”, sin necesidad de implementar controles adicionales, aunque se deben monitorear igualmente ante los cambios en el contexto externo e interno que puedan requerir la revisión del análisis realizado.

No obstante, los riesgos que superan el criterio de aceptación de la institución se deben administrar; por lo que el análisis aplicado es un insumo vital para la toma de decisiones; ya que con este conocimiento se pueden establecer los planes y estrategias para salvaguardar la vida de las personas y mitigar los impactos de un evento disruptivo en los procesos o servicios críticos del Poder Judicial.

La Guía de Implementación de la norma ISO 22301:2019 indica que:

*“El propósito de la norma no es necesariamente lograr la mitigación total del impacto de la interrupción, sino de ayudar a una organización a comprender la magnitud y el tipo de impacto que está dispuesta a aceptar después de una interrupción para lo cual la organización desarrolla un sistema de continuidad del negocio dimensionado correctamente para sus necesidades”.*

Un Sistema de Gestión de Continuidad del Servicio (SGCS) es una agrupación de métodos, procedimientos y normas interrelacionados para salvaguardar la continuidad de los procesos y servicios críticos o esenciales. La norma orienta a que el establecimiento del sistema da la capacidad a la organización para controlar, evaluar y continuar mejorando la continuidad del servicio.

Como parte del sistema, se establece la Gestión de la Continuidad del Servicio (GCS), que es el proceso de implementar y mantener la continuidad del servicio; con el fin de preparar a la organizaciónpara tratar incidentes disruptivos que, en caso contrario, podrían impedir el logro de sus objetivos (INTE ISO 22313-2015-SGCN Orientaciones).

Como parte del sistema opera la administración del riesgo, que en principio no procura evitar los riesgos, pues la gestión de la continuidad parte de la base de la materialización de estos, y a partir de ello, determinar la manera de responder a un incidente disruptivo y definir cómo continuar o recuperar las actividades dentro de un plazo predeterminado, a nivel aceptable.

El gráfico 2 muestra que ante un riesgo de disrupción inaceptable (según el apetito del riesgo institucional) se debe tener como prioridad la reducción del impacto. En gestión de la continuidad la identificación y análisis de riesgo permite a la organización tomar medidas a través de **estrategias de continuidad del servicio** que ayuden a prevenir los riesgos y reducir sus efectos (impacto). Este es el caso de:

* Planes de capacitación y rotación del personal para reducir las dependencias de personal crítico y anticipar medidas ante la ausencia o indisponibilidad del personal titular a cargo de los procesos o servicios críticos;
* Crear redundancias en los sistemas de información a través de contingencias en sitios de datos alternos;
* Dar formación a más personal informático que requiere especialización para dar soporte a procesos o servicios críticos de la institución o aplicar planes de revisión y pruebas a equipos sensibles que pueden afectar los sistemas de información;
* Robustecer las plataformas de seguridad para repeler ataques cibernéticos o fortalecer la inversión en hardware y software asociados a procesos y servicios críticos que dependen de tecnologías de información;
* Negociar acuerdos con terceros para anticipar lugares a dónde trasladar físicamente la prestación de servicios en caso de indisponibilidad de la infraestructura física habitual o
* Tomar medidas para la provisión regular de insumos de los cuales dependen procesos o servicios críticos; entre otras medidas de anticipación.

Por su parte, los **planes de continuidad del servicio** se orientan a responder a un incidente disruptivo y en establecer cómo continuar o recuperar las actividades dentro de un plazo predeterminado, en función del tipo de amenaza o escenario disruptivo. Por tanto, estos planes se elaboran con base en las estrategias y las soluciones seleccionadas para establecer los pasos inmediatos que se deben tomar durante una disrupción y se centran en el impacto de los incidentes que potencialmente conducen a ella.

Los planes de continuidad orientan sobre qué se debe hacer para proseguir y recuperar las actividades prioritarias, de manera que deben contener las instrucciones para saber en qué momento deben activarse los procedimientos para que las entregas de servicios se realicen de acuerdo con una capacidad previamente definida (INTE G130 2022\_Cor 2023); esto es, a un nivel aceptable, dentro de un plazo aceptable (trabajar en modo degradado)[[1]](#footnote-1).

Como tal, su propósito es mitigar el riesgo para reducir su impacto, de manera que se gestionen las consecuencias inmediatas de una disrupción y según lo establece la norma, contribuyan a prevenir de nuevas pérdidas ante la interrupción de la normalidad en la prestación de servicios.

### Gráfico 2. Tendencia del impacto de riesgos de continuidad ante medidas de administración.



**Fuente:** Elaboración propia a partir de modelos de gestión aplicables.

En otro sentido, la norma establece que la organización debe **implementar y mantener** un proceso de evaluación de riesgos. También establece que las evaluaciones de riesgos deben realizarse a periodos planificados o cuando se produzcan cambios significativos en la organización o en el contexto en el que opera (INTE G130 2022\_Cor 2023).

A nivel del Poder Judicial, esta gestión permanente debe incorporarse a la labor ordinaria de la oficina rectora en el SEVRI, que es la Oficina de Control Interno del Poder Judicial. En ese sentido, según acuerdo tomado por el Consejo Superior en la sesión 46-2023, celebrada el 1 de junio de 2023, artículo XLVI, esa Oficina debe:

*“Mantener dentro de su programación anual, las labores asociadas a la Gestión de Continuidad del Servicio, en cuanto a la identificación de riesgos asociados a procesos críticos y las gestiones que se deben desarrollar y llevar a cabo junto a las oficinas a cargo de esos procesos críticos, para el suministro de información necesaria en los planes del Sistema de Gestión de Continuidad del Servicio”*.

A su vez, cada oficina o despacho judicial y, de manera particular las que cuentan con procesos o servicios catalogados como críticos en el *“Análisis de Impacto al Servicio Institucional”*, debe incorporar el análisis de riesgos dentro de su propia gestión de la continuidad del servicio.

El gráfico 3 muestra de manera general esta interrelación entre los sistemas de gestión que van desde la operativa de la oficina a la gestión de la continuidad y la de riesgos

### Gráfico 3. Relación de modelos de gestión con la continuidad del servicio institucional.



**Fuente:** Elaboración propia a partir de normas y modelos de gestión aplicables.

Al respecto, debe tenerse en cuenta que la norma instruye a que en una primera etapa la organización debe identificar sus procesos y servicios críticos o esenciales; posteriormente, se debe aplicar la evaluación de riesgos de disrupción, con el fin de definir las estrategias y soluciones de continuidad, para finalmente formular (con esta información insumo) los planes de continuidad del servicio.

En esta lógica, la función de cada despacho y oficina judicial junto con la labor de la Oficina de Control Interno vienen a vincularse y aportar a la gestión de la continuidad institucional, que ha sido catalogado a nivel de la jerarquía institucional como un *“proceso institucional, de naturaleza crítica y estratégica dentro del Poder Judicial”.*

# **9. Tratamiento de riesgos de disrupción**

Cada oficina o despacho judicial con procesos críticos debe realizar su análisis particular de riesgos de disrupción, según las amenazas que le sean particulares, en función de los procesos o servicios críticos a su cargo.

El *“Instructivo para la elaboración del Sistema Específico de Valoración de Riesgo Institucional (SEVRI)”* de la Oficina de Control Interno (versión 2022) ofrece una guía práctica de cómo realizar esta labor. No obstante, con el fin de coadyuvar en este ejercicio, en el presente informe se aporta una matriz de ejemplo para orientar el tratamiento de riesgos de continuidad.

## Tabla 13. Ejemplo: Matriz de respuesta a riesgos de continuidad.

|  |  |  |  |
| --- | --- | --- | --- |
| **Riesgo / Escenario** | **Fuentes / Controles / Efectos** | **Respuesta** | **Responsable** |
| **Indisponibilidad del recurso humano** | **Fuentes** (a prevenir) |  |  |
| **Factor externo (FE):**Enfermedades contagiosas.  | **Prevenir:** * Aplicar medidas sanitarias para evitar contagios.
* Elaborar protocolos para atender situaciones de urgencia sanitaria.
 | Jefatura de la oficina.  |
| **Factor Humano (FH):**Enfermedad del personal capacitado o especializado. | **Prevenir:** * Capacitar al personal para que asuma diferentes funciones.
* Rotar funciones para que el personal conozca los diferentes puestos.
* Documentar procedimientos de trabajo y socializarlos con el personal.
* Establecer procedimiento para sustitución del personal.
* Elaborar procedimientos de continuidad para atender los procesos o servicios catalogados como críticos que se ven afectados por la ausencia del personal (puede implicar teletrabajo, refuerzo de personal de otras áreas o sedes, entre otras medidas).
 | Jefatura de la oficina. Subjefatura o puesto de Coordinación. |
| **Controles** (a mejorar) |  |  |
|  | * Actualización periódica de los manuales o procedimientos.
* Procedimientos de trabajo para los diferentes puestos actualizados.
* Verificación de la aplicación y funcionalidad de los planes ante situaciones simuladas (Pruebas y simulacros).
 | Jefatura de la oficina. Subjefatura o puesto de Coordinación. |
| **Efectos** (a mitigar) |  |  |
| **Factor Humano (FH):**Ausencia del personal responsable a cargo de procesos o servicios críticos. | **Mitigar*** Aplicar teletrabajo, como estrategia de continuidad del servicio.
* Ejecutar los procedimientos de continuidad para atender los procesos o servicios catalogados como críticos que se ven afectados por la ausencia del personal.
 | Jefatura de la oficina y todo el personal del despacho.  |
| **Indisponibilidad tecnológica total** | **Fuentes** |  |  |
| **Factor externo (FE):**Ataque cibernético. | **Prevenir:** * Diseñar y aplicar una política de respaldo de información crítica o esencial.
* Prever recursos necesarios para ejecutar procesos o servicios críticos, de manera manual (sin sistemas ni equipos).
* Diseñar planes de continuidad para la ejecución manual de los procesos o servicios críticos o indispensables.
* Socializar con todo el personal los planes diseñados para la continuidad del servicio.
 | Jefatura de la oficina. Subjefatura o puesto de Coordinación. |
| **Controles** |  |  |
|  | * Actualización periódica de los manuales o procedimientos.
* Procedimientos de trabajo para los diferentes puestos actualizados.
* Verificación de la aplicación y funcionalidad de los planes ante situaciones simuladas (Pruebas y simulacros).
 | Jefatura de la oficina. Subjefatura o puesto de Coordinación. |
| **Efectos** |  |  |
| Imposibilidad de acceder a los equipos de cómputo y a los sistemas de información.  | **Mitigar*** Ejecutar los procedimientos de continuidad para atender los procesos o servicios catalogados como críticos que se ven afectados por la indisponibilidad de sistemas o enlaces de comunicación.
 | Todo el personal de la oficina o despacho.  |
| **Indisponibilidad tecnológica parcial** | **Fuentes** |  |  |
| **Infraestructura tecnológica (IT):** Falla de los sistemas de o de los enlaces de comunicación. | **Prevenir:** * Diseñar y aplicar una política de respaldo de información crítica o esencial.
* Prever recursos necesarios para ejecutar procesos o servicios críticos, sin sistemas.
* Diseñar planes de continuidad para la ejecución manual de los procesos o servicios críticos o indispensables.
* Socializar con todo el personal los planes diseñados para la continuidad del servicio.
 | Jefatura de la oficina. Subjefatura o puesto de Coordinación. |
| **Controles** |  |  |
|  | * Actualización periódica de los manuales o procedimientos.
* Procedimientos de trabajo para los diferentes puestos actualizados.
* Verificación de la aplicación y funcionalidad de los planes ante situaciones simuladas (Pruebas y simulacros).
 | Jefatura de la oficina. Subjefatura o puesto de Coordinación. |
| **Efectos** |  |  |
| Imposibilidad de utilizar los sistemas de información.**Nota:** Sí es posible utilizar aplicaciones locales de los equipos.  | **Mitigar*** Ejecutar los procedimientos de continuidad para atender los procesos o servicios catalogados como críticos que se ven afectados por la imposibilidad de acceder a los sistemas de información.
 | Todo el personal de la oficina o despacho. |
| **Indisponibilidad de la infraestructura física** | **Fuentes** |  |  |
| **Factor externo (FE):**Inundación originada por desastres naturales.**Infraestructura física (IF):** Inundación por ruptura de tubería. | **Prevenir:** * Diseñar protocolos para atender situaciones de emergencia por inundación.
* Coordinar con la Administración y otras instancias para tomar la previsión de un lugar adecuado al cual trasladar de manera temporal y contingente los procesos o servicios críticos o esenciales.
* Formalizar acuerdos con terceros para contar con espacios físicos, para trasladar de manera temporal y contingente los procesos o servicios críticos o esenciales, en caso necesario.
* Prever recursos necesarios para ejecutar procesos o servicios críticos, de manera contingente en espacios alternos.
* Diseñar planes de continuidad para la continuidad de los procesos o servicios críticos, en caso de indisponibilidad del espacio físico.
* Socializar con todo el personal los planes diseñados para la continuidad del servicio en caso de indisponibilidad del espacio físico.
 | Jefatura de la oficina. Subjefatura o puesto de Coordinación. |
| **Controles** |  |  |
|  | * Actualización periódica de los manuales o procedimientos.
* Procedimientos de trabajo para los diferentes puestos actualizados.
* Verificación de la aplicación y funcionalidad de los planes ante situaciones simuladas (Pruebas y simulacros).
 | Jefatura de la oficina. Subjefatura o puesto de Coordinación. |
| **Efectos** |  |  |
| Imposibilidad de utilizar el espacio físico para la prestación de servicios.  | **Mitigar*** Ejecutar los procedimientos de continuidad para atender los procesos o servicios catalogados como críticos que se ven afectados por la indisponibilidad de la infraestructura física.
 | Todo el personal de la oficina o despacho. |
| **Dependencia de proveedores externos** | **Fuentes** |  |  |
| **Factor externo (FE):**Factores internacionales o locales de corte económico, social, político o tecnológico que inciden en la cadena logística de los proveedores o en los servicios que proveen (incluye información de otras instituciones públicas). | **Prevenir:** * Identificar proveedores de bienes o servicios asociados a procesos o servicios críticos.
* Identificar los insumos requeridos para los procesos y servicios críticos, que dependen de proveedores externos.
* Identificar los proveedores con mayor riesgo de incumplimiento en el suministro de bienes o servicios.
* Diseñar planes para la continuidad de los procesos o servicios críticos, en caso de posibles incumplimientos de proveedores externos.
 | Jefatura de la oficina. Subjefatura o puesto de Coordinación. |
| **Controles** |  |  |
|  | * Control o seguimiento al cumplimiento de proveedores.
* Actualización periódica de los manuales o procedimientos.
* Procedimientos de trabajo para los diferentes puestos actualizados.
* Verificación de la aplicación y funcionalidad de los planes ante situaciones simuladas (Pruebas y simulacros).
 | Jefatura de la oficina. Subjefatura o puesto de Coordinación. |
| **Efectos** |  |  |
| Carencia de bienes o servicios provistos por proveedores externos.  | **Mitigar*** Ejecutar los procedimientos de continuidad para atender los procesos o servicios catalogados como críticos que se ven afectados por la indisponibilidad de la infraestructura física.
 | Todo el personal de la oficina o despacho. |
| **Carencia de insumos** | **Fuentes** |  |  |
| **Factor externo/interno (FEI):**Imposibilidad de cualquier tipo para tramitar o ejecutar procedimientos de compra de insumos (sea presupuestaria, legal, de trámite, operativa, técnica, etc.).**Factor Externo (FE):**Incumplimiento de plazos de entrega de proveedores de insumos. | **Prevenir:** * Identificar insumos esenciales para los procesos y servicios críticos a cargo de la oficina o despacho.
* Identificar las causas que pueden provocar la carestía de dichos insumos.
* Establecer un stock de seguridad de los insumos indispensables.
* Diseñar planes para la continuidad de los procesos o servicios críticos, en caso de escasez de los insumos esenciales.
 | Jefatura de la oficina. Subjefatura o puesto de Coordinación. |
| **Controles** |  |  |
|  | * Control de inventario y de la obsolescencia de los insumos.
* Actualización periódica de los manuales o procedimientos.
* Verificación de la aplicación y funcionalidad de los planes ante situaciones simuladas (Pruebas y simulacros).
 | Jefatura de la oficina. Subjefatura o puesto de Coordinación. |
| **Efectos** |  |  |
| Imposibilidad de ejecutar los procedimientos por carecer de insumos esenciales. | **Mitigar*** Ejecutar los procedimientos de continuidad para atender los procesos o servicios catalogados como críticos que se ven afectados por la indisponibilidad de la infraestructura física.
 | Todo el personal de la oficina o despacho. |

Fuente: Elaboración propia aplicando la metodología del SEVRI-PJ de la Oficina de Control Interno.

Tal como se dijo al anteceder esta tabla, cada oficina debe aplicar este ejercicio a su particularidad, según los factores de riesgo que le afecten, para lo cual pueden tomar como referente el contenido de la tabla *“Tabla 6. Identificación de riesgos de continuidad en el Poder Judicial”* del presente informe.

# **10. Conclusiones**

En sesión del Consejo Superior número 48-2022, celebrada el 7 de junio de 2022, artículo LXXV (acuerdo confidencial), entre otros puntos, se avaló la conformación del *“Proceso de Gestión de Continuidad del Servicio”*, como un nuevo proceso institucional, de naturaleza crítica y estratégica dentro del Poder Judicial. Por su parte, la Ley General de Administración Pública en su artículo 4 establece la obligación de que todos los servicios públicos deben cumplir con principios y entre ellos *la continuidad del servicio*; además, el artículo 14 de la Ley General de Control Interno establece el deber del jerarca y de los titulares subordinados de analizar y valorar los riesgos y adoptar las medidas necesarias para disminuir el nivel de riesgo, en este caso sobre la interrupción del servicio público que presta el Poder Judicial.

En el presente análisis se determina el peso relativo de los riesgos de disrupción para las actividades priorizadas del Poder Judicial, según cuantificación aplicada a la identificación de riesgos realizada por las personas dueñas de procesos y servicios críticos en el *“Informe de Análisis de Riesgos de Continuidad del Servicio del Poder Judicial”*, aprobado por el Consejo Superior en la sesión 72-2020 celebrada el 16 de julio de 2020, artículo XIII.

A la ponderación de riesgos se incorpora la valoración según el conocimiento adquirido en el Poder Judicial con los recientes cambios en la organización y en el contexto, principalmente por la vivencia de la materialización de riesgos derivados del huracán Otto en el año 2016, la huelga del personal judicial en el año 2018, la pandemia ocasionada por el COVID-19 en el año 2020 y siguientes, la amenaza por ataques cibernéticos a instituciones públicas, así como otros riesgos de menor alcance, pero que también se han materializado (inundaciones, incidentes tecnológicos, cortes del suministro eléctrico, caídas de centros de datos, por ejemplo).

De esta manera, en este documento se consiga el resultado de la identificación de los riesgos de continuidad vinculados a los procesos y servicios institucionales que resultan críticos o esenciales para el Poder Judicial; a la vez que se categorizaron los distintos tipos de riesgos de continuidad, según escenarios de disrupción que podrían afectar al Poder Judicial.

Entre los principales resultados, se tienen:

* Se cuantifican 530 recurrencias de factores o fuentes de riesgo. Estos son, *elementos que solos o en combinación, tiene el potencial intrínseco para generar un riesgo* (ISO 31000).
* Los factores fueron agrupados, según su afectación, en cinco escenarios de riesgo: **a)** Indisponibilidad del Recurso Humano, **b)** Indisponibilidad de la infraestructura física, **c)** Indisponibilidad tecnológica, **d)** Dependencia de proveedores externos y **e)** Carencia de insumos.
* El escenario de “Indisponibilidad de la infraestructura física” recoge la mayor cantidad de recurrencias en diferentes factores, con un 44,3% del total de registros anotados. De este escenario, los daños por agua (8,5%) y desastres naturales (8,3%) son los factores de mayor recurrencia y cuentan con experiencias donde se han materializado. Les siguen en porcentaje de recurrencia las amenazas por ataques externos (8,1%), fuego (7,9%) y desastres industriales o en el espacio de trabajo (7,5%).

Según el análisis de riesgo inherente a nivel global para el escenario de Indisponibilidad de la infraestructura, este se clasifica como **Alto**, debido a que su ocurrencia es muy probable y su impacto es muy alto sobre la continuidad de los servicios institucionales.

* En porcentaje de importancia relativa sigue el escenario de “Indisponibilidad tecnológica” con un 31,5% de la recurrencia total de factores o fuentes de riesgos de disrupción identificados. En este escenario el corte de suministro eléctrico (8,1%), falla de servicios de comunicaciones (5,3%) y falla de sistemas o plataformas de operaciones (1,1%) se han materializado; pero también tienen una importancia muy significativa, por el riesgo que representan, las amenazas tecnológicas (7,5%) y el acceso no autorizado a la infraestructura tecnológica (6,8%).

Según el análisis de riesgo inherente a nivel global para el escenario de Indisponibilidad tecnológica, este se clasifica como **Alto**, debido a que su ocurrencia es muy probable y su impacto también es muy alto sobre la continuidad de los servicios institucionales.

* El escenario de “Indisponibilidad del recurso humano” agrupa el 14% de la recurrencia de los factores o fuentes de riesgo. En particular, la indisponibilidad o carencia del personal por sí solo concentra el 8,9% de las recurrencias y como bien es conocido a nivel institucional, es un riesgo materializado. A nivel de riesgo inherente se clasifica como **Alto** en virtud de la vital dependencia que los servicios institucionales tienen del factor y capital humano.

En este escenario también sobresalen la falta de personal capacitado o especializado y la indisponibilidad del personal informático asociado a procesos o servicios críticos y a la labor de mantener operativa la plataforma tecnológica. Al agrupar estos dos factores con el anterior, suman un 12,1% de las recurrencias en total, lo cual vuelve a resaltar la criticidad del personal a nivel institucional.

* Con una participación menor, pero no despreciable, emergen en este análisis (pues no se evidenciaron en el estudio realizado en el año 2020) los escenarios de riesgos de continuidad vinculados a la “Carencia de insumos” (6,2%) y la “Dependencia de proveedores externos” (4%).

Debido a que a nivel global tienen una probabilidad de ocurrencia menor y un impacto medio (pues algunos no afectan a todos los procesos o servicios críticos a nivel institucional) su riesgo inherente se clasifica como **Medio**.

En estos escenarios se ubican factores como falla de equipos base o soporte (aires acondicionados, alarmas, control de acceso), indisponibilidad de vehículos o transporte, carencia de equipos adecuado y necesario, falta de presupuesto, interrupción de servicios públicos básicos, incumplimiento de proveedores que incluye información o servicios provistos por otras instituciones públicas (Registro Nacional, Adaptación Social, Banco de Costa Rica, por ejemplo).

* Según el apetito al riesgo, la institución podría aceptar aquellos riesgos ubicados en los niveles “Muy bajo” y “Bajo”, sin necesidad de implementar controles adicionales, aunque se deben monitorear igualmente ante los cambios en el contexto externo e interno que puedan requerir la revisión del análisis realizado. No obstante, los riesgos que superan el criterio de aceptación de la institución se deben administrar; por lo que el análisis aplicado es un insumo vital para la toma de decisiones; ya que con este conocimiento se pueden establecer los planes y estrategias para salvaguardar la vida de las personas y mitigar los impactos de un evento disruptivo en los procesos o servicios críticos del Poder Judicial.
* *“El propósito de la norma no es necesariamente lograr la mitigación total del impacto de la interrupción, sino de ayudar a una organización a comprender la magnitud y el tipo de impacto que está dispuesta a aceptar después de una interrupción”* (ISO 22301:2019 Guía de Implementación)*.* Por tanto, en principio, no se procura evitar los riesgos, pues la gestión de la continuidad parte de la base de la materialización de estos, y a partir de ello, determinar la manera de responder a un incidente disruptivo y definir cómo continuar o recuperar las actividades dentro de un plazo predeterminado, a nivel aceptable. Esto se logra a través de **estrategias de continuidad del servicio** que ayuden a prevenir los riesgos y reducir sus efectos (impacto) y los **planes de continuidad del servicio** que guían en cómo responder a un incidente disruptivo y en establecer cómo continuar o recuperar las actividades dentro de un plazo predeterminado, en función del tipo de amenaza o escenario disruptivo; de manera que su propósito es mitigar el riesgo para reducir su impacto.
* La Norma establece que la organización debe **implementar y mantener** un proceso de evaluación de riesgos y también establece que las evaluaciones de riesgos deben realizarse a periodos planificados o cuando se produzcan cambios significativos en la organización o en el contexto en el que opera (INTE G130 2022\_Cor 2023). A nivel del Poder Judicial, esta gestión permanente debe incorporarse a la labor ordinaria de la oficina rectora en el SEVRI, que es la Oficina de Control Interno del Poder Judicial, según acuerdo tomado por el Consejo Superior en la sesión 46-2023, celebrada el 1 de junio de 2023, artículo XLVI
* A su vez, cada oficina o despacho judicial y, de manera particular las que cuentan con procesos o servicios catalogados como críticos en el *“Análisis de Impacto al Servicio Institucional”*, debe incorporar el análisis de riesgos dentro de su propia gestión de la continuidad del servicio.
* Finalmente, en este informe se aporta como ejemplo de aplicación para guiar a las oficinas y despachos judiciales en su gestión de la continuidad de procesos o servicios críticos, una matriz de muestra para orientar el tratamiento de riesgos de continuidad. Sin embargo, se aclara que cada oficina o despacho judicial con procesos críticos debe realizar su análisis particular de riesgos de disrupción, según las amenazas que le sean particulares, en función de los procesos o servicios críticos a su cargo.

# **11. Recomendaciones**

**Al Consejo Superior del Poder Judicial:**

* Aprobar el contenido del informe de *“Actualización de Análisis de Riesgos de Continuidad del Servicio del Poder Judicial”*, elaborado por el Subproceso de Gestión de Continuidad del Servicio del Poder Judicial, oficina adscrita a la Dirección Ejecutiva.
* Ordenar a la Oficina de Control Interno del Poder Judicial que incorpore los aspectos pertinentes contemplados en este informe dentro de su programación anual, según las labores asociadas a la Gestión de Continuidad del Servicio y la Gestión Institucional de Riesgos, en cuanto a la identificación de riesgos asociados a procesos críticos y las gestiones que se deben desarrollar y llevar a cabo junto a las oficinas a cargo de esos procesos críticos.

En ese mismo sentido, esa Oficina podría contemplar dentro de su labor, según lo que establece la Norma de continuidad de servicios y análisis de riesgos de continuidad, aspectos como:

* Definición de lineamientos para el establecimiento de controles y medidas para reducir la probabilidad de que ocurran los riesgos de continuidad y minimizar su impacto.
* Monitorear y revisar continuamente las estrategias de tratamiento del riesgo de continuidad, para asegurar su efectividad.
* Establecer un proceso de seguimiento continuo para supervisar la implementación de las estrategias de gestión de riesgos de continuidad.
* Ordenar a todas las oficinas y despachos judiciales, con especial énfasis en las que son dueñas de procesos o servicios críticos, que incorporen dentro de su revisión periódica del SEVRI-PJ el análisis de los factores y fuentes de riesgo contemplados en el presente informe, además de cualquier otro que sea particular a la oficina o despacho o que surjan como nuevas amenazas.

**A la Oficina de Control Interno:**

* Incorporar los aspectos contemplados en el presente informe en el *“Portafolio y Estructura de Riesgos Institucional”*, cuya última versión fue publicada en la Circular 264-2023 de la Secretaría General de la Corte, según lo aprobado por la Corte Plena en sesión 42-2023, celebrada el 11 de setiembre de 2023, artículo XXI.
1. Por definición, *“La continuidad del servicio es la capacidad de la organización para seguir suministrando productos o servicios* ***a niveles predefinidos y aceptables****, después de un incidente disruptivo” (INTE ISO 22313-2015-SGCN Orientaciones).* [↑](#footnote-ref-1)