



## **Plan de Continuidad de los Servicios**

**Unidad de Desarrollo Estratégico Institucional**

**Noviembre, 2024**



## PLAN DE CONTINUIDAD REGISTRO NACIONAL

### Unidad de Desarrollo Estratégico Institucional

#### Elaborado por

Nombre	Cargo	Firma
Paola Chavarría Agüero	Analista de Fortalecimiento Institucional	

#### Revisado por

Marcela Coto Garrido	Coordinadora a.i Subproceso Fortalecimiento Institucional	
----------------------	---	--

#### Aprobado por

Adelita Abarca Ortega	Jefe Unidad de Desarrollo Estratégico Institucional	
-----------------------	---	--

**Noviembre, 2024**



## Equipo de trabajo

Kattia Salazar Villalobos, Directora, Dirección de Servicios

Roger Araya Fonseca, Director, Dirección de Informática

Edwin Monge Alfaro, Subdirector, Dirección de Servicios

Carlos Obando Vargas, Jefe Departamento Financiero

Carlos López Vargas, Jefe Departamento Plataforma de Servicios

Fabiola Varela Mata. Jefa Departamento Recepción y Entrega

Gabriela Zúñiga Bermúdez, Jefa Departamento Proyección Institucional

Oscar Morales Segura, Jefe Departamento Aseguramiento de la Información

Roy Valenciano González, Jefe Departamento Infraestructura Tecnológica

Ericka Robles Rodríguez, Coordinadora Subproceso Entrega

Freddy Guido Calvo, Coordinador Subproceso Certificaciones

Geovanny Guevara Fernández, Coordinador Subproceso Recepción y notificación de Propiedad Intelectual

Mayra Camacho Méndez, Coordinadora Subproceso Placas

Zulema Rodríguez Castillo, Coordinadora Subproceso Recepción

Rosibel Zúñiga Richmond, Coordinadora Administrativa

Giovanni Fonseca Salas, Gestor de Salud Ocupacional



## Contenido

I.	Presentación.....	5
II.	ASPECTOS GENERALES .....	6
A.	Glosario.....	6
B.	Marco Jurídico .....	8
C.	Política de Continuidad de los Servicios .....	9
D.	Justificación .....	10
III.	DESARROLLO DEL PLAN DE CONTINUIDAD .....	12
A.	Metodología para la elaboración del Plan de Continuidad.....	12
B.	Objetivos .....	14
C.	Ámbito de aplicación .....	15
D.	Responsables y funciones .....	15
E.	Plazos para la recuperación de los servicios críticos, detalle de actividades y recursos .....	21
F.	Procedimientos .....	36
G.	Interdependencias internas y externas y sus interacciones .....	37
H.	Identificación de niveles de criticidad .....	41
I.	Tecnologías de información .....	44
J.	Recursos Financieros .....	48
K.	Mecanismos de información y comunicación.....	52
L.	Pruebas .....	52
M.	Documentación y lecciones aprendidas .....	53
N.	Compromiso institucional .....	54
O.	Seguimiento .....	54



## I. Presentación

Las instituciones públicas no se encuentran ajenas a que les ocurran eventos disruptivos, afectando con esto la prestación de los servicios a los usuarios. La capacidad para reponerse a estos eventos es esencial, principalmente como una medida para resguardar la vida de las personas funcionarias que conforman la Institución, sin descuidar la atención que se brinda a las personas usuarias, donde la no prestación de los servicios podría llevar a la pérdida de credibilidad, afectando con ello de manera directa su imagen y reputación.

En vista de lo anterior, y tomando como referencia las buenas prácticas desarrolladas por otras organizaciones, el Registro Nacional presenta a continuación el Plan de Continuidad, con el objetivo de definir los aspectos medulares a considerar en caso de que se presente un evento disruptivo, que de manera significativa afecte la atención de los servicios críticos que se brindan a los usuarios, mismo que define los aspectos medulares que se deben tener presentes en la Institución para la continuidad de los servicios.



## II. ASPECTOS GENERALES

### A. Glosario

**Aceptación del riesgo:** Decisión administrativa para no tomar ninguna acción de mitigación del impacto de un riesgo en particular.

**Activar:** Acto de declarar que las acciones definidas por la Institución sobre continuidad de los servicios deben llevarse a la práctica, con el fin de continuar con la prestación de sus servicios críticos, después de haberse materializado un incidente disruptivo.

**Análisis de Impacto a los Servicios, (por sus siglas en inglés BIA):** Proceso de análisis de las actividades y el efecto que la interrupción en la prestación de los servicios críticos podría tener sobre ellas.

**Análisis de requerimientos de continuidad:** Proceso de recopilar información en la fuente para reanudar y continuar las actividades de la institución a un nivel requerido para apoyar las obligaciones y objetivos de la organización

**Actividad:** Conjunto de tareas realizadas por una organización, para la producción de bienes o servicios.

**Activo:** Recurso que genera en el corto, mediano, o largo plazo un beneficio.

**Amenaza:** Causa potencial de un incidente no deseado que puede resultar en daños a individuos, activos, a un sistema u organización, el ambiente o la comunidad.

**Causa:** Condiciones concretas que originan el evento.

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

**Continuidad de los servicios:** Es la capacidad de la organización para continuar con la prestación de sus servicios críticos, después de haberse materializado un incidente disruptivo.



**Crisis:** Un incidente tiene la capacidad o el potencial de generar una crisis, se origina cuando un incidente impacta o podría impactar sobre la viabilidad, operatividad o credibilidad de la institución.

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

**Gestión de continuidad de los servicios:** Gestión enfocada a desarrollar en la organización la capacidad para continuar con la prestación de sus servicios críticos, después de haberse materializado un incidente disruptivo.

**Incidente disruptivo:** Evento o circunstancia que puede afectar significativamente las operaciones críticas de la organización. Esto incluye cualquier ocurrencia inesperada de causa natural, técnica o humana la cual representa una seria amenaza para el personal, clientes, instalaciones, activos, registros y/o oferta de servicios de la institución.

**Impacto:** Evento que tiene la capacidad de provocar la pérdida de o la interrupción de las operaciones, servicios o funciones de la organización, el cual, si no se administra, puede escalar y convertirse en una emergencia, crisis o desastre.

**Interrupción:** Evento que interrumpe las operaciones o procesos normales del negocio bien sea de manera anticipada (huracanes, inestabilidad política) o imprevista (bloqueos, ataques terroristas, fallas tecnológicas, o terremotos)

**Mitigación:** Se refiere a las acciones que se realizan para reducir el impacto o consecuencia del evento disruptivo.

**Objetivo:** Es el fin último hacia el cual se dirigen las acciones de una organización.

**Período máximo tolerable de interrupción, (por sus siglas en inglés MTPOD):** Es el tiempo que se tomaría para que los efectos adversos que pudieran ocurrir, como resultado de no proporcionar un producto/servicio o realizar una actividad lo convierta en inaceptable.

**Plan de Continuidad de los Servicios:** Se refieren a las acciones a realizar en la Institución para responder, continuar y recuperar los servicios críticos, después de haberse materializado un incidente disruptivo.



**Prevención:** Medidas contra amenazas específicas que habilitan a la organización evitar una interrupción de sus servicios.

**Recuperación:** La implementación gradual de las acciones definidas para volver a la normalidad en la prestación de los servicios.

**Respuesta a incidente:** Ejecutar acciones para minimizar el incidente materializado, destacando sus consecuencias, para posteriormente comunicarlas a los sujetos interesados que correspondan.

**Riesgo.** Probabilidad de que ocurran eventos que tendrían consecuencias sobre el cumplimiento de los objetivos fijados.

**Sistema de Gestión de Continuidad de los servicios (SGCS):** Comprende el conjunto de actividades que se deben realizar en el Registro Nacional para gestionar la prestación de los servicios de manera continua ante la presencia de un evento disruptivo.

**Servicios críticos:** Son aquellos que su entrega tiene una afectación o impacto directo en las partes interesadas considerados como prioritarios.

**Sujetos interesados:** Personas físicas o jurídicas, internas o externas a la Institución, que pueden ser afectadas directamente debido a la interrupción de los servicios.

**Tiempo objetivo de recuperación, (por sus siglas en inglés RTO):** Período de tiempo después de un incidente disruptivo en el que, el servicio debe ser reanudado.

**Valoración del riesgo:** consiste en la identificación, evaluación, selección y ejecución de medidas para la administración de riesgos.

## B. Marco Jurídico

A continuación, se presenta la normativa considerada en la realización de este documento:

- Ley de Creación del Registro Nacional, Ley N° 5695, del 28 de mayo de 1975 y sus reformas.



- Norma técnica de Costa Rica (INTECO) denominada INTE/ISO 22301:2015 Seguridad de la sociedad. Sistemas de gestión de continuidad del negocio. Requisitos.
- Sistemas de gestión de Continuidad de Servicios para organizaciones públicas y sin fines de lucro. Requisitos y orientación para su uso. INTE G 130: 2022.
- Normas técnicas para la gestión y el control de las Tecnologías de información, Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones, 2022.
- Directrices de continuidad para la generación de valor público en la Contraloría General de la República, R-DC-006-2021.
- Metodología de Gestión de la Continuidad de los Servicios SGCS, 2ºversión 2021, aprobado en el Acuerdo J147-2021, sesión N°10-2021, del 6 de mayo del 2021.
- Oficio MIDEPLAN-DM-OF-1595-2020, del 03 de diciembre del 2020.

## **C. Política de Continuidad de los Servicios**

### **I nivel**

El Registro Nacional se compromete a gestionar la continuidad en la prestación de los servicios que se determinen como críticos, ante la presencia de un evento disruptivo que los afecte.

### **II nivel**

#### Lineamientos

- En el Sistema de Gestión de la Continuidad de los Servicios (SGCS) se establece como prioritario las personas, los servicios críticos y la plataforma tecnológica que los soporta.
- El Sistema de Gestión de la Continuidad de los Servicios (SGCS), es aplicable a las instancias del Registro Nacional que tienen relación con los servicios críticos.



- La Institución dispone de un marco metodológico actualizado que orienta el funcionamiento del Sistema de Gestión de la Continuidad de los Servicios (SGCS) Sistema de Gestión de la Continuidad de los Servicios (SGCS).
- La Unidad de Desarrollo Estratégico Institucional (UDEI) es la instancia que coordina las acciones necesarias para la implementación y mantenimiento del Sistema de Gestión de la Continuidad de los Servicios (SGCS)
- La Dirección de Informática es la encargada de la recuperación de la plataforma tecnológica que soporta los servicios críticos.
- A los titulares subordinados responsables de los procesos sustantivos, les corresponde la identificación y definición de sus servicios críticos, así como la participación en la elaboración y ejecución, de los planes para prevenir, atender y evaluar los eventos que afecten la prestación de sus servicios.
- Al jerarca y titulares subordinados les corresponde identificar, analizar, evaluar, administrar y dar seguimiento a los riesgos relacionados con la continuidad de los servicios críticos, en apego a la metodología SEVRI definida en la Institución.
- El personal del Registro Nacional y de las organizaciones albergadas en la Institución, así como todo el personal de las empresas contratadas que brindan servicios a la Institución deben participar y ejecutar las acciones que se definan en materia de prevención y atención de eventos disruptivos.
- En toda contratación relacionada con los servicios críticos de la Institución, se debe solicitar al proveedor un plan de contingencia, ante un evento que interrumpa la continuidad de los servicios que presta, de conformidad con el objeto contractual.
- El Registro Nacional propicia la capacitación del personal involucrado en el desarrollo del SGCS, de acuerdo con la disponibilidad de los recursos.

#### **D. Justificación**

Las instituciones públicas en su accionar se pueden enfrentar a diferentes eventos disruptivos que afecten el cumplimiento de su operativa diaria, mismos que pueden impactar de manera total o parcial la continuidad de los servicios. En concordancia con las mejores prácticas



internacionales es fundamental que las entidades públicas desarrollen planes para que puedan dar respuesta ante posibles eventos que puedan ocasionar algún tipo de impacto en sus actividades. En tal sentido es de vital importancia que el Registro Nacional disponga de un Plan de Continuidad que contemple las acciones mínimas para garantizar la continuidad de los servicios críticos, facilitando la recuperación de estos cuando se hayan visto afectados por la incidencia de eventos disruptivos que impacten las operaciones esenciales.

Contar con este Plan permite a la Institución gestionar la recuperación de los servicios críticos, mantener la legitimidad institucional y mitigar el riesgo reputacional ante las partes interesadas, tomando en consideración las amenazas del entorno que podrían afectar la consecución de los objetivos. Asimismo, permite dar una respuesta a las necesidades de los usuarios ante la materialización de un evento, que pudieran generar un impacto en las actividades económico-sociales.

Por otro lado, es importante mencionar que en paralelo a la construcción de este plan se ha realizado la identificación y valoración de los riesgos, donde se han definido medidas de administración para mitigar su materialización.

En diversas evaluaciones o procesos de fiscalización, se ha indicado la necesidad de disponer de un Plan de Continuidad de los Servicios. Algunos de los documentos que hace referencia a este requerimiento son:

- Índice de Capacidad de la Gestión.
- Directrices de continuidad para la generación de valor público en la Contraloría General de la República, R-DC-006-2021.
- Normas técnicas para la gestión y el control de las Tecnologías de Información, MICITT.
- Normas técnicas de Costa Rica (INTECO), denominadas INTE/ISO 22301:2015, Seguridad de la sociedad. Sistemas de Gestión de continuidad del negocio. Requisitos.



### III. DESARROLLO DEL PLAN DE CONTINUIDAD

Referente al tema de Continuidad de los Servicios en el Registro Nacional, el Ministerio de Planificación Nacional y Política Económica, indica en el oficio MIDEPLAN-DM-OF-1595-2020, del 03 de diciembre del 2020, las funciones asignadas a la Unidad de Desarrollo Estratégico Institucional, mencionando como función la de: Coordinar acciones para el fortalecimiento del Sistema de Gestión de Continuidad de los Servicios del Registro Nacional.

En este contexto, la Unidad de Desarrollo Estratégico Institucional, en coordinación con otras instancias del Registro Nacional, ha logrado desarrollar importantes acciones relacionadas a la concretización del tema de continuidad, para lo cual dispone de los siguientes documentos:

- Diagnóstico
- Política de Continuidad de los Servicios.
- Análisis de la plataforma y los servicios tecnológicos que soportan los servicios críticos de la Institución.
- Metodología del Sistema de Gestión de la Continuidad de los servicios, 2º versión.
- Guía para el Desarrollo del Sistema de Gestión de Continuidad de los servicios en el Registro Nacional.
- Definición de los servicios críticos del Registro Nacional.
- Actualización Metodología de SEVRI, 8º versión en el cual se incluye como factor de riesgo el tema de Continuidad.
- Definición de los riesgos de continuidad e inclusión en el Sistema de SEVRI.
- Definición de procedimientos para la atención de eventos disruptivos.
- Inicio y aplicación de simulacros.

#### A. Metodología para la elaboración del Plan de Continuidad

La metodología utilizada para desarrollar este documento tomó en consideración una serie de aspectos los cuales se citan a continuación:



- **Investigación:** Con el fin de ampliar conocimientos en materia de Continuidad de los servicios, se procedió a realizar investigación en fuentes, públicas y privadas, donde se identificaron aspectos básicos y relevantes que debía contener un Plan de Continuidad. Producto de esta investigación se determinaron los contenidos del presente documento.
- **Entrevistas:** Se realizaron entrevistas a personas funcionarias vinculadas con la materia de continuidad en cada una de sus instituciones, entre ellas: Banco Nacional, Banco Popular, Empresa de Servicios Públicos de Heredia, Poder Judicial, la Contraloría General de la República. Esto permitió conocer la experiencia desarrollada y las lecciones aprendidas durante el proceso para garantizar la efectividad de un Plan de Continuidad.
- **Ánalisis de documentación:** Se analizó la normativa dispuesta en el Marco Normativo de este documento, con el propósito de adoptar y adaptar aquellos requerimientos que fuesen posibles desarrollar en la Institución para disponer del Plan de Continuidad, Plan de Contingencia y el Plan de Comunicación.
- **Definición de puntos básicos:** Para la elaboración de este documento, así como los demás planes que se elaboraron, se tomó en consideración lo establecido en la Norma técnica de Costa Rica (INTECO) denominada INTE/ISO 22301:2015 Seguridad de la sociedad. Sistemas de gestión de continuidad del negocio. Requisitos, así como, en el documento denominado Sistemas de gestión de Continuidad de Servicios para organizaciones públicas y sin fines de lucro. Requisitos y orientación para su uso. INTE G 130: 2022 y directrices de entes rectores como el MICITT y la Contraloría General de la República.

Asimismo, se recurrió a la participación de instancias que tienen vinculación directa en el tema de Continuidad como lo son la Dirección de Servicios, Dirección de Informática y el Departamento de Financiero, mismos que participaron activamente en la revisión de este documento y desarrollo de aspectos vinculados con la materia de su competencia.



- Redacción del documento: Para la redacción de los planes, se realizaron diversas reuniones con el equipo facilitador de la UDEI, para lo cual se tomó en consideración el análisis realizado con anterioridad a la normativa, la revisión de los conceptos básicos, el conocimiento obtenido de la experiencia de otras instituciones, lográndose culminar con la elaboración de este documento.

## B. Objetivos

### Objetivo General

Gestionar la continuidad de los servicios críticos prioritarios del Registro Nacional para dar respuestas oportunas a las necesidades de las personas usuarias ante la materialización de un evento disruptivo.

### Objetivos específicos:

- Mitigar los efectos de los daños o fallas por medio de la ejecución de un conjunto de acciones previamente definidas e informadas para el abordaje de la recuperación de los servicios.
- Establecer los requerimientos de recuperación de TI, Recursos Humanos, materiales y suministros para los servicios críticos ante la presencia de un evento disruptivo.
- Definir los actores involucrados en la prestación de los servicios críticos, así como sus funciones ante la materialización de un evento disruptivo que afecte la continuidad de los servicios.
- Establecer para cada servicio crítico el detalle de actividades a realizar, así como los tiempos requeridos para su implementación.



- Identificar los procedimientos asociados a los servicios críticos.

### **C. Ámbito de aplicación**

Este Plan aplica a los servicios críticos definidos como prioritarios para el Registro Nacional, donde se involucra a las personas funcionarias que tienen relación directa en la prestación de estos para garantizar la continuidad de los servicios ante incidentes disruptivos. En ese sentido, es importante mencionar que los servicios críticos definidos como prioritarios son los siguientes:

Servicios críticos:

1. Mantener disponibles los servicios de placas de manera presencial.
2. Mantener disponibles los servicios de placas en el portal web.
3. Mantener disponibles las consultas y certificaciones de manera presencial.
4. Mantener disponibles las consultas y certificaciones en el portal web.
5. Recepción, anotación, entrega y notificación de documentos digitales (ventanilla digital y WIPO-file).
6. Recibir, asignar citas de presentación, digitalizar, anotar, realizar el reparto, entregar y notificar los documentos físicos de BI, BM, PJ, y PI.
7. Recibir los documentos físicos calificados de los registradores (digitalizar, archivar y entregar/ notificar los documentos).
8. Traslado de documentos y placas a las diferentes regionales.

### **D. Responsables y funciones**

Con el propósito de tener claridad respecto a los responsables en materia de la Continuidad de los servicios críticos definidos en este documento, así como de las funciones que deben desempeñar para llevar a cabo las acciones que se requieren en la recuperación de los servicios, se presenta a continuación la siguiente información:



**Tabla 1**

*Responsables y funciones asignadas*

RESPONSABLES	FUNCIONES
Junta Administrativa	<ul style="list-style-type: none"><li>• Aprobar la Política de Continuidad de los Servicios.</li><li>• Aprobar la metodología sobre la continuidad de los Servicios.</li><li>• Aprobar el Plan de Continuidad de los Servicios.</li><li>• Apoyar la ejecución del Plan de Continuidad de los Servicios.</li></ul>
Director General	<ul style="list-style-type: none"><li>• Apoyar la ejecución de los objetivos y planes para el Sistema de Gestión de Continuidad de los Servicios, verificando que sean revisados anualmente.</li><li>• Aprobar las funciones y responsabilidades definidas a los actores involucrados en la continuidad de los servicios, antes, durante y después de materializarse un evento disruptivo.</li><li>• Solicitar informes sobre las revisiones y valoraciones correspondientes en el tema de Continuidad a la instancia que coordina acciones en la materia.</li><li>• Definir los tiempos para la ejecución de las actividades necesarias para restaurar los servicios.</li><li>• Realizar la convocatoria de las personas funcionarias involucradas en la coordinación de acciones para la continuidad de los servicios.</li><li>• Realizar la vocería oficial ante medios de comunicación, usuarios y poderes del estado.</li><li>• Brindar los lineamientos generales en la atención de eventos disruptivos.</li><li>• Aprobar la estrategia de comunicación para la atención en ante un evento disruptivo.</li><li>• Autorizar los comunicados que se hagan a nivel interno y externo en el tema de Continuidad de los servicios.</li><li>• Apoyar las gestiones que se realicen para llevar a cabo el Plan de Comunicación.</li></ul>



RESPONSABLES	FUNCIONES
Director de Informática	<ul style="list-style-type: none"><li>• Evaluar los daños relacionados a las TIC.</li><li>• Responder ante la convocatoria que realice la Dirección General en materia de continuidad de los servicios.</li><li>• Atender de acuerdo con su capacidad cuando se requiera ante la presencia de un evento disruptivo.</li><li>• Disponer de un plan de recuperación ante la presencia de eventos disruptivos que afecten los servicios críticos para cumplir con los objetivos de recuperación trazados por la Institución.</li><li>• Formar parte del equipo de personas funcionarias que se avoquen a la recuperación de los servicios críticos con la activación del plan de continuidad.</li><li>• Coordinar acciones de supervisión en el proceso de recuperación para la continuidad de los servicios.</li></ul>
Director de Servicios	<ul style="list-style-type: none"><li>• Responder ante la convocatoria de la DG.</li><li>• Ser el responsable sustituto el Jefe de Departamento Plataforma de Servicios, Departamento de Recepción y Entrega.</li><li>• Velar por la aplicación de los procedimientos establecidos, ante la presencia de un evento disruptivo.</li><li>• Coordinar con otras instancias la gestión de los recursos requeridos para la atención del servicio crítico.</li><li>• Coordinar con la Dirección de Informática funcionamiento de sistemas requeridos en los servicios críticos.</li><li>• Preparar los informes que le sean requeridos en materia de continuidad de los servicios.</li></ul>
Directores de Registros	<ul style="list-style-type: none"><li>• Contribuir con el proceso de continuidad de los servicios desde la identificación de los servicios críticos.</li><li>• Participar en los simulacros relacionados con la continuidad de los servicios.</li><li>• Comunicar a las partes involucradas las gestiones a realizar ante la disrupción de los servicios institucionales.</li><li>• Responder ante la convocatoria de la DG.</li></ul>



RESPONSABLES	FUNCIONES
	<ul style="list-style-type: none"><li>• Convocar a los funcionarios requeridos para la atención de la situación.</li><li>• Coordinar el trabajo dirigido a la atención del servicio crítico.</li><li>• Gestionar los recursos requeridos para la atención del servicio crítico.</li><li>• Comunicar resultados de la atención del servicio crítico.</li><li>• Verificar que el proceso registral de ejecute correctamente.</li></ul>
Jefe de Departamento Plataforma de Servicios, y Jefe Departamento de Recepción y Entrega	<ul style="list-style-type: none"><li>• Organizar el equipo de trabajo.</li><li>• Coordinar con las instancias correspondientes que los sistemas informáticos funcionan según los requerimientos de la situación.</li><li>• Gestionar los materiales y suministros necesarios para realizar las funciones en atención al servicio crítico.</li><li>• Verificar que el procedimiento vinculado al servicio crítico se ejecute correctamente.</li><li>• Brindar informes sobre la atención del servicio crítico.</li></ul>
Directora Administrativa	<ul style="list-style-type: none"><li>• Asumir en ausencia del director general o subdirector la coordinación para la atención de cualquier evento disruptivo.</li><li>• Monitorear el evento disruptivo, determinando su impacto, información que debe ser compartida a la Dirección General.</li><li>• Responder ante la convocatoria de la DG.</li><li>• Atender de acuerdo con su capacidad cuando se requiera ante la presencia de un evento disruptivo.</li><li>• Coordinar para corroborar el estado de la infraestructura física posterior a una situación disruptiva de los servicios.</li><li>• Coordinar la gestión de los recursos físicos, económicos y humanos para la atención de los servicios críticos.</li></ul>
Jefe Servicios Generales	<ul style="list-style-type: none"><li>• Asumir en ausencia de la persona que ocupe la Dirección General, Subdirección y Dirección Administrativa, la coordinación para la atención de cualquier evento disruptivo.</li><li>• Atender de acuerdo con su capacidad cuando se requiera ante la presencia de un evento disruptivo.</li></ul>



RESPONSABLES	FUNCIONES
	<ul style="list-style-type: none"><li>• Coordinar los aspectos relacionados con la infraestructura institucional.</li><li>• Coordinar de revisión de instalaciones electromecánicas.</li><li>• Realizar las coordinaciones necesarias para permitir accesos en los edificios.</li><li>• Establecer las coordinaciones necesarias para facilitar el uso de vehículos en la atención de eventos disruptivos.</li><li>• Gestionar la disponibilidad de personal relacionado con contratos de limpieza, seguridad, servicios de mantenimiento y otros que sean necesarios.</li><li>• Activar los protocolos de seguridad física institucional.</li></ul>
Unidad de Desarrollo Estratégico Institucional	<ul style="list-style-type: none"><li>• Responder ante la convocatoria de la DG.</li><li>• Revisar los documentos elaborados periódicamente en materia de continuidad de los servicios que garanticen la mejora continua.</li><li>• Mantener acopio de la documentación en materia de continuidad de los servicios.</li><li>• Coordinar los simulacros de atención de los servicios críticos.</li><li>• Vigilar la adecuada implementación de los procedimientos de la atención de servicios críticos.</li><li>• Verificar la ejecución del plan de atención de los servicios críticos.</li><li>• Actualizar la documentación relacionada con la Continuidad de los Servicios.</li><li>• Gestionar la implementación del Plan de Continuidad.</li></ul>
Departamento de Proyección Institucional	<ul style="list-style-type: none"><li>• Responder ante la convocatoria de la DG.</li><li>• Atender ante la presencia de un evento disruptivo, de acuerdo con su capacidad.</li><li>• Definir la estrategia de comunicación para la atención ante un evento disruptivo.</li><li>• Garantizar la disponibilidad de los medios de comunicación durante un incidente disruptivo.</li></ul>



RESPONSABLES	FUNCIONES
	<ul style="list-style-type: none"><li>• Ejecutar el plan de comunicación en materia de continuidad de los servicios.</li><li>• Mantener actualizado el plan de comunicación en concordancia con las necesidades institucionales y la normativa vigente.</li></ul>
Salud Ocupacional	<ul style="list-style-type: none"><li>• Responder ante la convocatoria de la DG.</li><li>• Atender ante la presencia de un evento disruptivo, de acuerdo con su capacidad.</li><li>• Mantener actualizado el plan de emergencia ante la presencia de un evento disruptivo que afecte la integridad física de las personas.</li><li>• Verificar que las condiciones laborales en la atención de los servicios críticos garantizan la seguridad laboral de los funcionarios.</li><li>• Denunciar riesgos de los funcionarios que atienden los servicios críticos ante condiciones inadecuadas.</li><li>• Proponer alternativas ante ausencia de seguridad laboral.</li></ul>
Personas funcionarias con tareas asignadas para la atención del servicio crítico.	<ul style="list-style-type: none"><li>• Responder ante la convocatoria del Superior Inmediato.</li><li>• Atender ante la presencia de un evento disruptivo, de acuerdo con su capacidad.</li><li>• Atender los lineamientos definidos por la Dirección General cuando se presente un evento disruptivo que afecte la prestación de los servicios críticos.</li><li>• Conocer sobre el plan de continuidad que se defina en la Institución para su ejecución cuando sea requerido.</li></ul>
Registradores	<ul style="list-style-type: none"><li>• Responder ante la convocatoria del Superior Inmediato.</li><li>• Verificar las adecuadas condiciones del espacio físico asignado.</li><li>• Verificar el funcionamiento de los sistemas.</li><li>• Verificar el funcionamiento del equipo tecnológico.</li><li>• Iniciar la calificación de documentos.</li><li>• Participar en reuniones para mejorar el proceso.</li></ul>

**Nota:** Elaboración UDEI.



## E. Plazos para la recuperación de los servicios críticos, detalle de actividades y recursos

A continuación, se presenta para cada servicio crítico, el detalle de las actividades para gestionarse la materialización de un evento disruptivo, así como la definición de las personas involucradas, los recursos requeridos para levantar los servicios y los sistemas que se necesiten estén en funcionamiento para la continuidad del servicio.

**Tabla 2**

*Servicio crítico: 1. Mantener disponibles los servicios de placas de manera presencial*

ACTIV.	TIEMPO EN HORAS	COORD.	RESP	RECURSOS	OTROS RECURSOS	SISTEMAS REQUERIDOS
1.1. Reunión inicial con los funcionarios responsables del servicio crítico para coordinar acciones de levantamiento.	1	Dirección General	Dirección General/Dirección de Servicios/Dirección de Informática /Dirección Administrativa	Personal de la Dirección de Servicios, Personal de la Dirección de Informática, Dirección General y Subdirector, personal del Departamento de Servicios Generales, Jefe de subproceso	Centro Alterno de Datos Servicios básicos: electricidad, internet, disponibilidad de sistemas, agua, transporte. Máquina para la confección de placas, insumos especiales	Sistemas SIBIMU, SIPLA, E-POWER, SPJ y los webservice (COSEVI, DNN, INS, Registro Civil).
<b>1.2. Análisis de daños:</b>	2					
1.2.1 Elaboración de un Plan de Trabajo para atender los daños y re establecer el servicio.		Se define en la reunión inicial dependiendo del incidente	Dirección General/Dirección de Servicios/Dirección de Informática /Dirección Administrativa	Personal de la Dirección de Servicios, Personal de la Dirección de Informática, Dirección General y Subdirector, personal del	Personal de la Dirección de Servicios, Personal de la Dirección de Informática, Dirección General y Subdirector, personal del	



ACTIV.	TIEMPO EN HORAS	COORD.	RESP	RECURSOS	OTROS RECURSOS	SISTEMAS REQUERIDOS
				Departamento de Servicios Generales, Jefe de subproceso	4 Computadoras 4 Estaciones de trabajo 1 impresora de punto de venta, 1 troqueladora 1 estampadora en calor 1 impresora de dispositivos de ID	
<b>1.3 Ejecutar el Plan para recuperar el servicio</b>	10					
1.3.1 Infraestructura TI		Director de Informática	Jefes de Departamentos de la DIN	Personal de la Dirección de Informática		
1.3.2 Infraestructura física		Director Administrativo	Jefatura Dpto. Servicios Generales	Personal del Departamento de Servicios Generales		
<b>1.4. Pruebas de funcionamiento</b>	3		Personal del subproceso.			
1.4.1 Pruebas de Troquelado		Jefe de Departamento de Plataforma de servicios	Coordinador Subproceso de Placas	Personal de la Dirección de Servicios/Personal del Subproceso de Placas/Personal Dirección de Informática		
1.4.2 Pruebas de pintura						
1.4.3 Pruebas en la APP						
<b>1.5. Elaboración de comunicado a la persona usuaria sobre la afectación del servicio (va en paralelo con las pruebas de)</b>		Director General	Jefe del Departamento de Proyección	Dirección General y Personal de Proyección.		



ACTIV.	TIEMPO EN HORAS	COORD.	RESP	RECURSOS	OTROS RECURSOS	SISTEMAS REQUERIDOS
funcionamiento)						
	<b>16</b>					

**Nota:** Elaboración UDEI y Dirección de Servicios

**Tabla 3**

*Servicio crítico: 2. Mantener disponibles los servicios de placas en el portal web.*

ACTIV.	TIEMPO EN HORAS	COORD.	RESP	RECURSOS	OTROS RECURSOS	SISTEMAS REQUERIDOS
2.1. Reunión inicial con los funcionarios responsables del servicio crítico para coordinar acciones de levantamiento.	1	Dirección General	Dirección General/ Dirección de Servicios/ Dirección de Informática/ Dirección Administrativa	Personal de la Dirección de Servicios, Personal de la Dirección de Informática, Dirección General y Subdirector, personal del Departamento de Servicios Generales, Jefe del Subproceso.	Centro Alterno de Datos Servicios básicos: electricidad, internet, disponibilidad de sistemas, agua, transporte. Máquina para la confección de placas, insumos especiales para la confección de placas (chapas, stickers, cintas de estampado en calor, portafolios, dados, papel térmico)	Portal Institucional, SIBIMU, SIPLA, E-POWER, SISTEMA DE PAGOS DEL BCR, SPJ y los webservice (COSEVI, DNN, INS, Registro Civil).
<b>2.2. Análisis de daños:</b>	2					
2.2.1 Elaboración de un Plan de Trabajo para atender los daños y re establecer el servicio		Se define en la reunión inicial dependiendo del incidente	Dirección General/ Dirección de Servicios/ Dirección de Informática/ Dirección Administrativa	Personal de la Dirección de Servicios, Personal de la Dirección de Informática, Dirección General y Subdirector, personal del Departamento de Servicios Generales	Personal de la Dirección de Servicios, Personal de la Dirección de Informática, Dirección General y Subdirector, personal del Departamento de Servicios Generales	4



ACTIV.	TIEMPO EN HORAS	COORD.	RESP	RECURSOS	OTROS RECURSOS	SISTEMAS REQUERIDOS
<b>2.3 Ejecutar el Plan para recuperar el servicio</b>	10				Computadoras 4 Estaciones de trabajo 1 impresora de punto de venta, 1 troqueladora 1 estampadora en calor 1 impresora de dispositivos de ID	
2.3.1 Infraestructura TI		Director de Informática	Jefes de Departamentos de la DIN	Personal de la Dirección de Informática		
2.3.2 Infraestructura física		Director Administrativo	Jefatura dep Servicios Generales	Personal del Departamento de Servicios Generales		
<b>2.4. Pruebas de funcionamiento</b>	3		Personal del subproceso			
2.4.1 Pruebas para verificar que el enlace del Ministerio de Hacienda y el Banco Central de CR con el sistema de PJ esté en funcionamiento		Jefe de Departamento de Plataforma de servicios	Coordinador Subproceso de Placas.	Personal de la Dirección de Servicios/ATR Dirección de PJ/Dirección de Informática		
<b>2.5. Elaboración de comunicado a la persona usuaria sobre la afectación del servicio (va en paralelo con las pruebas de funcionamiento)</b>		Director General	Jefe del Departamento de Proyección	Dirección General y Personal de Proyección.		
	<b>16</b>					

**Nota:** Elaboración UDEI y Dirección de Servicios



**Tabla 4**

*Servicio crítico:3. Mantener disponibles las consultas y certificaciones de manera presencial*

ACTIV.	TIEMPO EN HORAS	COORD.	RESP.	RECURSOS	OTROS RECURSOS	SISTEMAS REQUERIDOS
3.1. Reunión inicial con los funcionarios responsables del servicio crítico para coordinar acciones de levantamiento.	1	Dirección General	Dirección General/Dirección de Servicios/Dirección de Informática	Personal de la Dirección de Servicios, Personal de la Dirección de Informática, Dirección General y Subdirector, personal del Departamento de Servicios Generales, Jefe del Subproceso	Centro Alterno de Datos Servicios básicos: electricidad, internet, agua, transporte. 5 Computadoras 5 impresoras 5 estaciones de trabajo, sistemas sustantivos y papel para impresión.	Se requiere de los sistemas sustantivos de todos los Registros.
<b>3.2 Análisis de daños:</b>	2					
3.2.1 Elaboración de un Plan de Trabajo para atender los daños y re establecer el servicio		Se define en la reunión inicial dependiendo del incidente	Dirección General/Dirección de Servicios/Dirección de Informática	Personal de la Dirección de Servicios, Personal de la Dirección de Informática, Dirección General y Subdirector		
<b>3.3 Ejecutar el Plan para recuperar el servicio</b>	8					
3.3.1 Infraestructura TI		Dirección de Informática	Jefes de Departamentos de la DIN	Personal de la Dirección de Informática		



ACTIV.	TIEMPO EN HORAS	COORD.	RESP.	RECURS OS	OTROS RECURSOS	SISTEMAS REQUERIDOS
<b>3.4. Pruebas de funcionamiento</b>	5					
3.4.1 Pruebas de Consultas		Jefe de Departamento de Plataforma de servicios	Jefe del Subproceso de Certificaciones	Personal de la Dirección de Servicios. Personal de la Dirección de informática, Mesa de ayuda.		
3.4.2 Pruebas certificaciones						
3.4.3 Pruebas de Impresoras						
<b>3.5. Elaboración de comunicado a la persona usuaria sobre la afectación del servicio (va en paralelo con las pruebas de funcionamiento)</b>		Dirección General	Jefe del Departamento de Proyección	Dirección General y Personal de Proyección.		
	<b>16</b>					

**Nota:** Elaboración UDEI y Dirección de Servicios



**Tabla 5**

*Servicio critico: 4. Mantener disponibles las consultas y certificaciones en el portal web*

ACTIV.	TIEMP O EN HORA S	COORD.	RESP.	RECURS OS	OTROS RECURSOS	SISTEMAS REQUERIDOS
4.1. Reunión inicial con los funcionarios responsables del servicio crítico para coordinar acciones de levantamiento.	1	Dirección General	Dirección General/Dirección de Servicios/Dirección de Informática	Personal de la Dirección de Servicios, Personal de la Dirección de Informática, Dirección General y Subdirector, personal del Departamento de Servicios Generales; Jefe del Subproceso	Centro Alterno de Datos Servicios básicos: electricidad, internet, agua, transporte. 2 Computadoras, 2 estaciones de trabajo para atención de consultas a través de la webmaster, servidores informáticos y bases de datos.	Portal Institucional, SIBIMU, SPJ, SIRE, SIRI, SIP, IPAS, SEC, SIPLA, E-POWER, SISTEMA DE PAGOS DEL BCR.
<b>4.2 Análisis de daños:</b>	2					
4.2.1 Elaboración de un Plan de Trabajo para atender los daños y re establecer el servicio		Se define en la reunión inicial dependiendo del incidente	Dirección General/Dirección de Servicios/Dirección de Informática	Personal de la Dirección de Servicios, Personal de la Dirección de Informática, Dirección General y Subdirector		
<b>4.3 Ejecutar el Plan para recuperar el servicio</b>	8					
4.3.1 Infraestructura TI		Dirección de Informática	Jefes de Departamentos de la DIN	Personal de la Dirección de Informática		
<b>4.4. Pruebas de funcionamiento</b>	5					



ACTIV.	TIEMPO EN HORAS	COORD.	RESP.	RECURSOS	OTROS RECURSOS	SISTEMAS REQUERIDOS
4.4.1 Pruebas de Consultas al sistema de Personas jurídicas		Jefe de Departamento de Plataforma de servicios	Gestor de servicios	Personal de la Dirección de Servicios		
<b>4.5. Elaboración de comunicado a la persona usuaria sobre la afectación del servicio (va en paralelo con las pruebas de funcionamiento)</b>		Dirección General	Jefe del Departamento de Proyección	Dirección General y Personal de Proyección.		
	<b>16</b>					

**Nota:** Elaboración UDEI y Dirección de Servicios

## Tabla 6

*Servicio critico:5. Recepción, anotación, entrega y notificación de documentos digitales (Ventanilla digital y WIPO-file)*

ACTIV.	TIEMPO EN HORAS	COORD	RESP.	RECURSOS	OTROS RECURSOS	SISTEMAS REQUERIDOS
5.1. Reunión inicial con los funcionarios responsables del servicio crítico para coordinar acciones de levantamiento.	1	Dirección General	Dirección General/Dirección de Servicios/Dirección de Informática/Dirección Administrativa	Personal de la Dirección de Servicios, Personal de la Dirección de Informática, Dirección general y Subdirector, Jefe Departamento.	Sistema de recepción 8 Computadoras Conexión a internet.	Ventanilla digital, WIPO File, SIDU, SIRE, SPJ, SIBIMU, SIP, IPAS, componente de firma digital, web services: DNN, Registro Civil.



ACTIV.	TIEMPO EN HORAS	COORD	RESP.	RECURSOS	OTROS RECURS OS	SISTEMAS REQUERID OS
<b>5.2. Análisis de daños:</b>	2					
5.2.1 Elaboración de un Plan de Trabajo para atender los daños y re establecer el servicio		Se define en la reunión inicial dependiendo del incidente	Dirección General/Dirección de Servicios/Dirección de Informática	Personal de la Dirección de Servicios, Personal de la Dirección de Informática, Dirección General y Subdirector		
<b>5.3 Ejecutar el Plan para recuperar el servicio</b>	8					
5.3.1 Infraestructura TI		Director de Informática	Jefes de Departamentos de la DIN	Personal de la Dirección de Informática		
5.3.2 Infraestructura física		Director Administrativo	Jefatura Dpto. Servicios Generales	Personal del Departamento de Servicios Generales		
<b>5.4. Pruebas de funcionamiento</b>	5					
5.4.1. Pruebas de al sistema SIBIMU, SIRE, SPJ, IPAS, WIPO-File		Coordinador del Subproceso de Recepción /ATRS de los registros sustantivos.	ATRS de los registros sustantivos. / Jefe de Departamento de Recepción y Entrega/Coordinador de Subproceso de Recepción,	Personal de la Dirección de Informática y Dirección de Servicios		
5.4.2. Pruebas de visualización de los documentos			Coordinador Subproceso de Recepción y notificación de PI, Coordinador Subproceso de Entrega.			
5.4.3. Pruebas de Anotación						
5.4.4. Pruebas de reparto						
5.4.5. Pruebas de entrega						
5.4.6. Pruebas de notificación						



ACTIV.	TIEMPO EN HORAS	COORD	RESP.	RECURSOS	OTROS RECURSOS	SISTEMAS REQUERIDOS
<b>5.5. Elaboración de comunicado a la persona usuaria sobre la afectación del servicio (va en paralelo con las pruebas de funcionamiento)</b>		Dirección General	Jefe del Departamento de Proyección	Dirección General y Personal de Proyección.		
	<b>16</b>					

**Nota:** Elaboración UDEI y Dirección de Servicios

**Tabla 7**

*Servicio critico: 6. Recibir, asignar citas de presentación, digitalizar, anotar, realizar el reparto, entregar y notificar los documentos físicos de BI, BM, PJ, y PI*

ACTIVIDAD	TIEMPO EN HORAS	COORD.	RESP.	RECURSOS	OTROS RECURSOS	SISTEMAS REQUERIDOS
6.1. Reunión inicial con los funcionarios responsables del servicio crítico para coordinar acciones de levantamiento.	1	Dirección General	Dirección General/Dirección de Servicios/Dirección de Informática /Dirección Administrativa	Personal de la Dirección de Servicios, Personal de la Dirección de Informática, Dirección General y Subdirector, Jefe de Departamento.	Sistema de recepción 8 computadoras Conexión a internet, multifuncional, escáner y conexión a internet.	SIDU, SIRE, SPJ, SIBIMU, SIP, IPAS, E-POWER, E-SCAN.
<b>6.2. Análisis de daños:</b>	2					
.2.1 Elaboración de un Plan de Trabajo para atender los daños y		Se define en la reunión inicial dependiendo del incidente	Dirección General/Dirección de Servicios/Dirección de Informática /Dirección	Personal de la Dirección de Servicios, Personal de la Dirección de Informática,		



ACTIVIDAD	TIEMPO EN HORAS	COORD.	RESP.	RECURSOS	OTROS RECURSOS	SISTEMAS REQUERIDOS
reestablecer el servicio			Administrativa	Dirección General y Subdirector, personal del Departamento de Servicios Generales		
<b>6.3 Ejecutar el Plan para recuperar el servicio</b>	8					
6.3.1 Infraestructura TI		Director de Informática	Jefes de Departamentos de la DIN	Personal de la Dirección de Informática		
6.3.2 Infraestructura física		Director Administrativo	Jefatura Dpto. Servicios Generales	Personal del Departamento de Servicios Generales		
<b>6.4. Pruebas de funcionamiento</b>	5					
6.4.1. Pruebas de recepción		Coordinador del Subproceso de Recepción /ATRS de los registros sustantivos,	ATR /Jefe de Departamento de Recepción y entrega/Coordinador de Subproceso de Recepción, Coordinador Subproceso de Recepción y notificación de PI, Coordinador Subproceso de Entrega.	Personal de la Dirección de Informática y Servicios		
6.4.2. Pruebas de visualización de los documentos						
6.4.3. Pruebas de Anotación						
6.4.4. Pruebas de reparto						
6.4.5. Pruebas de entrega						
6.4.6. Pruebas de notificación						



ACTIVIDAD	TIEMPO EN HORAS	COORD.	RESP.	RECURSOS	OTROS RECURSOS	SISTEMAS REQUERIDO S
<b>6.5. Elaboración de comunicado a la persona usuaria sobre la afectación del servicio (va en paralelo con las pruebas de funcionamiento)</b>		Dirección General	Jefe del Departamento de Proyección	Dirección General y Personal de Proyección.		
	<b>16</b>					

**Nota:** Elaboración UDEI y Dirección de Servicios

## Tabla 8

*Servicio critico:7. Recibir los documentos calificados de los registradores (digitalizar, archivar y entregar/notificar los documentos)*

ACTIV.	TIEMPO EN HORAS	COORD.	RESP.	RECURSOS	OTROS RECURSOS	SISTEMAS REQUERIDOS
7.1. Reunión inicial con los funcionarios responsables del servicio crítico para coordinar acciones de levantamiento.	1	Dirección General	Dirección General/ Dirección de Servicios/ Director de Informática	Personal de la Dirección de Servicios, Personal de la Dirección de Informática, Dirección General y Subdirector, personal del Departamento de Servicios Generales,	Sistemas 3 Computadoras Conexión a internet, 1 impresora, 1 escáner	SIRE, SPJ, SIBIMU, SIP, IPAS, E-POWER, E-SCAN.



ACTIV.	TIEMPO EN HORAS	COORD.	RESP.	RECURSOS	OTROS RECURSOS	SISTEMAS REQUERIDOS
				Jefe de Subproceso		
<b>7.2 Análisis de daños:</b>	2					
7.2.1 Elaboración de un Plan de Trabajo para atender los daños y re establecer el servicio		Se define en la reunión inicial dependiendo del incidente	Dirección General/ Dirección de Servicios/ Dirección de Informática	Personal de la Dirección de Servicios, Personal de la Dirección de Informática, Dirección General y Subdirector		
<b>7.3 Ejecutar el Plan para recuperar el servicio</b>	8					
7.3.1 Infraestructura TI		Dirección de Informática	Jefes de Departamentos de la DIN	Personal de la Dirección de Informática		
<b>7.4. Pruebas de funcionamiento</b>	5					
7.4.1 Pruebas del sistema SIRE (Sistema de Registro Inmobiliario), sistemas sustantivos		Jefe de Departamento de Recepción y entrega	Subproceso de Entrega/ ATRS de registros sustantivos/ Informática	Personal de la Dirección de Servicios		
<b>7.5. Elaboración de comunicado a la persona usuaria sobre la afectación del servicio (va en paralelo con las pruebas)</b>		Dirección General	Jefe del Departamento de Proyección	Dirección General y Personal de Proyección.		



ACTIV.	TIEMPO EN HORAS	COORD.	RESP.	RECURSOS	OTROS RECURSOS	SISTEMAS REQUERIDOS
<b>de funcionamie nto)</b>						
	<b>16</b>					

**Nota:** Elaboración UDEI y Dirección de Servicios

**Tabla 9**

*Servicio critico:8. Traslado de documentos y placas a las diferentes Regionales*

ACTIV.	TIEMPO EN HORAS	COORD.	RESP.	RECURSOS	OTROS RECURSOS	SISTEMAS REQUERIDOS
8.1. Reunión inicial con los funcionarios responsables del servicio crítico para coordinar acciones de levantamiento.	1	Dirección General	Dirección General/Dirección de Servicios/Dirección de Informática	Personal de la Dirección de Servicios, Personal de la Dirección de Informática, Dirección General y Subdirector, personal del Departamento de Servicios Generales, Jefe de Subproceso.	Sistemas 1 Computadora Conexión a internet, 1 impresora	SIRE, SPJ, SIBIMU, SIP, E-POWER, E-SCAN.
<b>8.2 Análisis de daños:</b>	2					
8.2.1 Elaboración de un Plan de Trabajo para atender los daños y re establecer el servicio		Se define en la reunión inicial dependiendo del incidente	Dirección General/Dirección de Servicios/Dirección de Informática	Personal de la Dirección de Servicios, Personal de la Dirección de Informática		



ACTIV.	TIEMPO EN HORAS	COORD.	RESP.	RECURS OS	OTROS RECURSOS	SISTEMAS REQUERIDOS
				, Dirección General y Subdirector		
<b>8.3 Ejecutar el Plan para recuperar el servicio</b>	8					
8.3.1 Infraestructur a TI		Director de Informáti ca	Jefes de Departame ntos de la DIN	Personal de la Dirección de Informática		
<b>8.4. Pruebas de funcionamie nto</b>	5					
8.4.1 Servicio de transporte del Registro Nacional		Jefe de Departam ento de Recepción y Entrega	Coordinado r Subproceso de Entrega/Jef e de Servicios Generales	Personal de la Dirección de Servicios/ Personal del Departame nto de Servicios Generales		
<b>8.5. Elaboración de comunicado a la persona usuaria sobre la afectación del servicio (va en paralelo con las pruebas de funcionamie nto)</b>		Director General	Jefe del Departame nto de Proyección	Dirección General y Personal de Proyección.		
	<b>16</b>					

**Nota:** Elaboración UDEI y Dirección de Servicios



## F. Procedimientos

Con la finalidad de disponer del paso a paso a desarrollar en caso de presentarse un evento disruptivo, se definieron procedimientos para facilitar la ejecución de las acciones que permitan dar continuidad a los servicios afectados.

De acuerdo con los servicios críticos identificados se presenta a continuación los siguientes procedimientos:

**Tabla 10**

*Procedimiento por servicio crítico*

<b>Servicio crítico</b>	<b>Código procedimiento</b>	<b>Nombre procedimiento</b>
1. Mantener disponibles los servicios de placas de manera presencial.	DSE-PSE-023	Recuperación del servicio de placas ante un evento disruptivo.
2. Mantener disponibles los servicios de placas en el portal web.	DSE-PSE-023	Recuperación del servicio de placas ante un evento disruptivo.
3. Mantener disponibles las consultas y certificaciones de manera presencial.	DSE-PSE-024	Recuperación del servicio de consultas y certificaciones ante un evento disruptivo.
4. Mantener disponibles las consultas y certificaciones en el portal web.	DSE-PSE-024	Recuperación del servicio de consultas y certificaciones ante un evento disruptivo.



<b>Servicio critico</b>	<b>Código procedimiento</b>	<b>Nombre procedimiento</b>
5. Recepción, anotación, entrega y notificación de documentos digitales (Ventanilla digital y WIPO-file).	DSE-REN-013	Recuperación del servicio de recepción, anotación, entrega y notificación de documentos digitales (ventanilla digital y wipo file) ante un evento disruptivo.
6. Recibir, asignar citas de presentación, digitalizar, anotar, realizar el reparto, entregar y notificar los documentos físicos de BI, BM, PJ, y PI.	DSE-REN-014	Recuperación del servicio de recepción, asignación de citas de presentación, digitalización, anotación y reparto de documentos físicos ante un evento disruptivo.
7. Recibir los documentos calificados de los registradores (digitalizar, archivar y entregar/notificar los documentos).	DSE-REN-015	Recuperación del servicio de recepción, digitalización y archivo de documentos físicos calificados por los registradores, así como su entrega y notificación ante un evento disruptivo.
8. Traslado de documentos y placas a las diferentes Regionales.	DSE-REN-016	Recuperación del servicio de traslado de documentos y placas a las diferentes sedes regionales ante un evento disruptivo.

**Nota:** Elaboración UDEI y Dirección de Servicios

## **G. Interdependencias internas y externas y sus interacciones**

La continuidad del servicio exige de la generación de métodos, procedimientos y normas interrelacionados con el objetivo de disminuir la afectación en la prestación de los servicios definidos como críticos. En ese sentido, conocer las interrelaciones que tienen los servicios



críticos definidos como prioritarios para Registro Nacional, tanto con las empresas externas, como las relaciones que ocurren a lo interno, es fundamental, dado a que una afectación en uno de los servicios críticos generaría un efecto en cadena en distintos ámbitos.

Seguidamente, se detallan estas interrelaciones en las que se vinculan los servicios críticos a nivel externo e interno:

**Tabla 11**

*Interdependencia externa e interna de los servicios críticos*

Servicio	Relación externa	Relación interna
1. Mantener disponibles los servicios de placas de manera presencial	<ul style="list-style-type: none"><li>* Consejo de Seguridad Vial (COSEVI)</li><li>* Revisión Técnica Vehicular DEKRA</li><li>* Instituto Nacional de Seguros (INS)</li><li>* Aseguradoras de vehículos</li><li>* Agencias de vehículos</li><li>* Correos de Costa Rica</li><li>* Ministerio de Hacienda-TICA</li><li>* Consejo de Transporte público (CTP)</li><li>* Entidades financieras</li><li>* Personas físicas y jurídicas</li><li>* Banco de Costa Rica (BCR)</li><li>* Organismo de Investigación Judicial (OIJ)</li><li>* Tribunal Supremo de Elecciones (TSE)</li><li>* Dirección Nacional de Notariado (DNN)</li><li>* Convenio de Adaptación Social</li><li>* Instituciones públicas</li><li>* Adjudicatario de Contrataciones</li></ul>	<ul style="list-style-type: none"><li>* Dirección General</li><li>* Dirección de Servicios</li><li>* Departamento Plataforma de Servicios</li><li>* Subproceso Placas</li><li>* Subproceso de Recepción</li><li>* Sedes Regionales</li><li>* Subproceso de Entrega</li><li>* Dirección de Informática</li><li>* Departamento Servicios al Usuario de Tecnología de la Información (Mesa de Ayuda)</li><li>* Departamento de Desarrollo de Soluciones</li><li>* Dirección de Bienes Muebles</li><li>* Dirección de Personas Jurídicas</li><li>* Dirección Administrativa</li><li>* Contraloría de Servicios</li><li>* Departamento de Servicios Generales</li><li>*</li></ul>



Servicio	Relación externa	Relación interna
2. Mantener disponibles los servicios de placas en el portal web	<ul style="list-style-type: none"><li>* Consejo de Seguridad Vial (COSEVI)</li><li>* Revisión Técnica Vehicular (DEKRA)</li><li>* Instituto Nacional de Seguros (INS)</li><li>* Aseguradoras de vehículos</li><li>* Agencias de vehículos</li><li>* Correos de Costa Rica</li><li>* Ministerio de Hacienda-TICA</li><li>* Consejo de Transporte público (CTP)</li><li>* Entidades financieras</li><li>* Personas físicas y jurídicas</li><li>* Banco de Costa Rica (BCR)</li><li>* Organismo de Investigación Judicial (OIJ)</li><li>* Tribunal Supremo de Elecciones (TSE)</li><li>* Dirección Nacional de Notariado (DNN)</li><li>* Adaptación Social</li><li>* Instituciones públicas</li><li>* Adjudicatario de Contrataciones</li></ul>	<ul style="list-style-type: none"><li>* Dirección General</li><li>* Dirección de Servicios</li><li>* Departamento Plataforma de Servicios</li><li>* Subproceso Placas</li><li>* Subproceso de Recepción</li><li>* Subproceso de Entrega</li><li>* Sedes Regionales</li><li>* Dirección de Informática</li><li>* Departamento Servicios al Usuario de Tecnología de la Información (Mesa de Ayuda)</li><li>* Departamento de Desarrollo de Soluciones</li><li>* Dirección de Bienes Muebles</li><li>* Dirección de Personas Jurídicas</li><li>* Dirección Administrativa</li><li>* Contraloría de Servicios</li><li>* Departamento de Servicios Generales</li></ul>
3. Mantener disponibles las consultas y certificaciones de manera presencial	<ul style="list-style-type: none"><li>* Personas físicas y jurídicas</li><li>* Banco de Costa Rica (BCR)</li><li>* Ministerio de Hacienda</li><li>* Dirección Nacional de Notariado (DNN)</li><li>* Tribunal Supremo de Elecciones (TSE)</li><li>* Banco Central de Costa Rica</li></ul>	<ul style="list-style-type: none"><li>* Dirección General.</li><li>* Dirección de Bienes Muebles.</li><li>* Dirección de Personas Jurídicas</li><li>* Dirección Inmobiliario</li><li>* Departamento de Normalización Técnica</li><li>* Instituto Geográfico Nacional</li><li>* Dirección Propiedad Intelectual</li><li>* Dirección de Servicios</li><li>* Departamento de Recepción y Entrega</li><li>* Departamento de Plataforma de Servicios</li><li>* Sedes Regionales</li><li>* Subprocesos de Normalización Técnica de cada Registro sustantivo</li><li>* Dirección de Informática</li></ul>



Servicio	Relación externa	Relación interna
4. Mantener disponibles las consultas y certificaciones en el portal web	<ul style="list-style-type: none"><li>* Personas físicas y jurídicas</li><li>* Banco de Costa Rica (BCR)</li><li>* Ministerio de Hacienda</li><li>* Dirección Nacional de Notariado (DNN)</li><li>* Tribunal Supremo de Elecciones (TSE)</li><li>* Banco Central de Costa Rica</li></ul>	<ul style="list-style-type: none"><li>* Dirección General</li><li>* Dirección de Servicios</li><li>* Departamento de Plataforma de Servicios</li><li>* Departamento de Recepción y Entrega</li><li>* Sedes Regionales</li><li>* Dirección de Bienes Muebles.</li><li>* Dirección de Personas Jurídicas</li><li>* Dirección Inmobiliario</li><li>* Departamento de Normalización Técnica</li><li>* Instituto Geográfico Nacional</li><li>* Dirección Propiedad Intelectual</li><li>* Dirección de Informática</li><li>* Subprocesos de Normalización Técnica de cada Registro sustantivo</li><li>* Proyección Institucional</li><li>* Asesoría Jurídica</li></ul>
5. Recepción, anotación, entrega y notificación de documentos digitales (Ventanilla digital y WIPO-file)	<ul style="list-style-type: none"><li>* Banco de Costa Rica (BCR)</li><li>* Dirección Nacional de Notariado (DNN)</li><li>* Banco Central de Costa Rica (BCCR)</li><li>* Personas físicas y jurídicas</li><li>* Tribunal Supremo de Elecciones (TSE)</li><li>* Organización Mundial de Propiedad Intelectual (OMPI).</li></ul>	<ul style="list-style-type: none"><li>* Dirección de Servicios</li><li>* Departamento de Recepción y entrega</li><li>* Sedes Regionales</li><li>* Dirección de Bienes Muebles.</li><li>* Dirección de Personas Jurídicas</li><li>* Dirección Inmobiliario</li><li>* Departamento de Normalización Técnica</li><li>* Dirección Propiedad Intelectual</li><li>* Subprocesos de Normalización Técnica de cada Registro sustantivo</li><li>* Dirección de Informática.</li></ul>
6. Recibir, asignar citas de presentación, digitalizar, anotar, realizar el reparto, entregar y notificar los documentos físicos de BI, BM, PJ, y PI.	<ul style="list-style-type: none"><li>* Personas físicas y jurídicas</li><li>* Tribunal Supremo de Elecciones (TSE)</li><li>* Organización Mundial de Propiedad Intelectual (OMPI)</li><li>* Banco de Costa Rica (BCR)</li><li>* Correos de Costa Rica</li></ul>	<ul style="list-style-type: none"><li>* Dirección de Servicios</li><li>* Departamento de Recepción y entrega</li><li>* Sedes Regionales</li><li>* Dirección de Bienes Muebles.</li><li>* Dirección de Personas Jurídicas</li><li>* Dirección Inmobiliario</li><li>* Departamento de Normalización Técnica</li><li>* Dirección Propiedad Intelectual</li><li>* Subprocesos de Normalización Técnica de cada Registro sustantivo</li><li>* Dirección de Informática</li></ul>



Servicio	Relación externa	Relación interna
7. Recibir los documentos calificados de los registradores (digitalizar, archivar y entregar/notificar los documentos).		*Dirección de Servicios * Departamento de Recepción y Entrega * Sedes Regionales *Dirección de Bienes Muebles. *Dirección de Personas Jurídicas *Dirección Inmobiliario *Dirección Propiedad Intelectual * Dirección de Informática
8. Traslado de documentos y placas a las diferentes Regionales	*Correos de Costa Rica	*Dirección General *Dirección de Servicios *Departamento de Plataforma de Servicios * Subproceso de Placas * Departamento de Recepción y Entrega * Sedes Regionales *Dirección de Bienes Muebles. *Dirección de Personas Jurídicas *Dirección Inmobiliario *Dirección Propiedad Intelectual * Dirección de Informática * Depto. Servicios Generales

**Nota:** Elaboración UDEI y Dirección de Servicios

## H. Identificación de niveles de criticidad

Identificar el nivel de criticidad es importante para determinar las acciones a desarrollar, tomando en consideración todos los escenarios que podrían desencadenar una situación no deseada.

Algunas de las situaciones que podrían afectar a la Institución son: desastres naturales, amenazas de usuarios molestos, atentados terroristas, desastres y pandemias. En este caso el equipo de gestión de crisis pueda controlar cómo reaccionar ante los acontecimientos. A continuación, la descripción de los niveles de criticidad.



### **Nivel Bajo:**

Se considera nivel bajo en aquellos casos en que la materialización del evento no paraliza la prestación de los servicios críticos. En este sentido, a pesar de presentarse un evento, este no afecta la cotidianidad de la operación y tiene un bajo impacto de a las personas usuarias.

Se consideran escenarios de nivel bajo los siguientes:

- Ausencia o incapacidad de un funcionario clave.
- Errores humanos en la gestión de los recursos para la prestación de servicios.
- Reubicaciones de funcionarios por remodelaciones o por reorganizaciones administrativas.
- Equipo de usuario final no disponible.

### **Nivel medio**

En este nivel los servicios críticos están teniendo una afectación de forma leve, implicando que sea lenta la prestación de los servicios críticos, por lo que la comunicación en este nivel se hará para los funcionarios involucrados y usuarios, esto podría provocar filas de espera y quejas de los usuarios.

Se consideran escenarios de nivel bajo los siguientes:

- Daño parcial en la infraestructura física que imposibilite el normal funcionamiento.
- Degrado en la operación de los aplicativos de software.
- Manifestaciones sociales externas.
- Actos vandálicos.



## Nivel alto

En el nivel alto, se da una gran afectación en la operatividad institucional y en la prestación del servicio a la persona usuaria, los medios de comunicación requieren explicación sobre la situación presentada, se necesita la intervención del responsable de emitir el comunicado oficial, las personas usuarias presentan sus inconformidades por diferentes medios incluyendo las redes sociales que trasciende a la opinión pública, los medios de comunicación requieren respuesta de los eventos ocurridos.

Se consideran escenarios de nivel alto los siguientes:

- Ausencia de personas funcionarias responsables de atender los servicios críticos en gran proporción.
- Fallo en el sistema de suministro eléctrico (servicio público, UPS, planta eléctrica).
- Daños graves en la infraestructura física que imposibilite el normal funcionamiento.
- Eventos naturales declarados como alerta por la Comisión Nacional de Emergencia para la protección de las personas.
- Centro de datos no se encuentra disponible.
- Caída de los servicios de telecomunicaciones.
- Suspensión o caída de los aplicativos de software.
- Terrorismo (artefactos explosivos, toma de rehenes e instalaciones).
- Fallo en la disponibilidad de la información requerida para la prestación de los servicios críticos.
- Incidentes de seguridad de la información.
- Huelga de los funcionarios del Registro Nacional.

A continuación, se detallan las acciones de comunicación que se implementarán en cada uno de los niveles de criticidad.



**Tabla 12**

*Características de comunicación de acuerdo con los niveles de criticidad*

<b>Nivel bajo</b>	<b>Nivel Medio</b>	<b>Nivel alto</b>
<ul style="list-style-type: none"><li>• La crisis atrae poca o ninguna atención.</li><li>• Se recibe la información antes de que el evento suceda.</li><li>• Las partes involucradas desconocen la afectación.</li></ul>	<ul style="list-style-type: none"><li>• La situación aún no se ha convertido en crisis.</li><li>• Los partes realizan consultas sobre la situación presentada.</li><li>• Los usuarios conocen de la situación o evento, pero no le prestan atención.</li></ul>	<ul style="list-style-type: none"><li>• Los medios de comunicación indagan sobre la situación presentada en el Registro.</li><li>• Se necesita la intervención del vocero oficial.</li><li>• Los usuarios expresan quejas verbales e indignación por medio de redes sociales o noticieros.</li></ul>

**Nota:** Elaboración UDEI

## **I. Tecnologías de información**

Las previsiones en aspectos sobre tecnologías de información tienen presentes los siguientes elementos:

### **I.1. Capacidad de la plataforma tecnológica**

Los departamentos de la Dirección de Informática han definido los protocolos para evaluar, de manera anual, la capacidad de la plataforma tecnológica que está bajo su gestión. Estos se



aplican en el cuarto trimestre del año, para lo cual se prepara un informe sobre el desempeño de la plataforma y se toman las consideraciones presupuestarias para mantener vigente la plataforma, acorde con las necesidades institucionales.

Periódicamente se realiza un análisis sobre componentes críticos de la plataforma tecnológica, con la finalidad de evaluar el porcentaje de esos componentes que cuentan con esquemas de alta disponibilidad y/o contingencia. Esta medida forma parte de las valoraciones que se realizan en la gestión del riesgo, denominada: “Incidentes y problemas en la prestación de los servicios de TI”.

## **I.2. Prevención de ataques ciberneticos**

En la aplicación de la metodología de riesgos (SEVRI), se encuentra identificado el evento “Afectación en la seguridad de los activos de información”. Por medio del análisis de este se gestiona de manera razonable, la exposición a ataques ciberneticos implementando las siguientes medidas:

- Análisis y atención de las alertas de seguridad que emite el MICITT.
- Aplicación de la normativa de aseguramiento de la información, incluyendo el Manual de normas de Aseguramiento de la Información y la Metodología de clasificación de activos de la información.
- Implementación del protocolo de respuesta a incidentes de seguridad de la información.
- Operación de herramientas de seguridad lógica.
- Definición y aplicación de procedimientos y guías del Departamento de Aseguramiento de la Información.
- Gestión de redes inalámbricas no autorizadas.
- Revisión de equipos especiales con conectividad (Troqueladora de placas, televisiones inteligentes, cámaras de seguridad, entre otros).



- Actualización permanente de versiones y firmware, cuando son liberados por los fabricantes.

Un factor muy importante, en la previsión de ataques ciberneticos, es la capacidad de las personas funcionarias para reconocer amenazas de ciberseguridad y proceder de acuerdo con las instrucciones que se han definido para esas situaciones. En ese sentido, se tiene el Manual de Normas de Aseguramiento de la Información, aprobado por la Junta Administrativa, y el cual se actualiza de manera periódica. También, se realizan estudios para observar la respuesta del personal ante situaciones sospechosas, se refuerzan las capacidades a través de cursos de concientización y constantemente, se utilizan los medios de comunicación oficiales para enviar recordatorios sobre estos temas.

### **I.3. Monitoreo de la plataforma tecnológica**

En cuanto al desempeño de los servicios, los departamentos de la Dirección de Informática designan a las personas funcionarias responsables de documentar las eventuales suspensiones de los servicios, mismas que presentan un informe mensual sobre el desempeño de los servicios.

Referente a las herramientas de seguridad se aplican los siguientes monitoreos:

- Intentos de accesos irregulares y de tráfico malicioso proveniente de redes externas, a través de los firewalls perimetrales.
- Prevención de intrusiones a través de la solución de IPS, además de análisis de tráfico irregular proveniente de diferentes países y bloqueos en caso de identificar intentos de ataques.
- Monitoreo de acceso a Internet y generación de bloqueos y restricciones a sitios catalogados como maliciosos.
- Detección de software malicioso y generación de cuarentenas de posibles archivos con virus.



- Bloqueo de tráfico irregular y malicioso hacia soluciones web que brindan los servicios del Registro Nacional.
- El MICITT mantiene también un monitoreo constante, a través del cual se detectan actividades y tráfico irregular desde y hacia el Registro Nacional, lo cual es notificado por parte de esa institución, a fin de que se tomen las acciones correspondientes.

Para monitorear los equipos de redes y telecomunicaciones se utiliza un contrato de monitoreo externo, al cual el Registro Nacional le define los componentes a considerar, los indicadores y los umbrales; esto se está revisando constantemente para ir ajustándolo a las necesidades de la Institución que puedan ir surgiendo. Además, se cuenta con herramientas de software que permiten monitorear el estado de la plataforma de redes y telecomunicaciones. Para los equipos que están fuera del alcance del monitoreo remoto, se utiliza una herramienta interna con indicadores y umbrales.

Para la gestión de las bases de datos se cuenta con un contratista para mantenimiento preventivo y correctivo de las bases de datos ORACLE, el cual realiza revisiones diarias de la salud de las bases de datos. Los servidores de BD son monitoreados como parte del contrato de monitoreo remoto.

#### **I.4. Satisfacción de necesidades de las partes interesadas (internas y externas)**

Los compromisos de la Dirección de Informática, en cuanto a la satisfacción de necesidades de las partes interesadas, están descritas en los **Acuerdo de Nivel de Servicio para la función de tecnologías de información y comunicaciones (SLA)**. Este documento es suscrito entre las Direcciones de Registro Nacional (clientes de los servicios) y la Dirección de Informática (proveedora de los servicios).

En los SLA se detalla la **Operatividad de Servicios en Línea** incluyendo la disponibilidad, la capacidad, la continuidad, la fiabilidad y la forma de evaluar el desempeño del servicio.



## **I.5. Plan de continuidad y recuperación de los servicios críticos de TI**

Con la finalidad de contar con formas alternas para la prestación de los servicios de TI (incluyendo partes externas interesadas) ante fallas de conectividad y otras circunstancias de índole técnico, se estableció el Plan de continuidad y recuperación de los servicios críticos de TI, detalla el protocolo para la recuperación de los servicios, señalando los roles y las actividades previas, durante y posteriores a los incidentes.

En este plan se describen las medidas tecnológicas para procurar la continuidad de los servicios de TI, considerando la operación en un centro de datos TIER III, redundancia y alta disponibilidad para componentes críticos, estrategia de virtualización, esquemas de respaldo de la información, redundancia de enlaces de telecomunicaciones, mecanismos para el balanceo de transacciones, utilización de recursos de nube (para lo que resulta aplicable), soluciones especializadas para la gestión del almacenamiento y herramientas de ciberseguridad (filtrado de contenido, antivirus, muros de fuego, muros de fuego para aplicaciones web).

## **J. Recursos Financieros**

### **J.1. Mecanismos de control del riesgo patrimonial**

Respecto a los mecanismos de control de riesgo patrimonial, el Registro Nacional cuenta con distintas pólizas de seguros, las cuales garantizan la atención de las personas en caso de accidente, además, prevé la reparación o reposición de activos como vehículos o equipo electrónico en caso de accidente o robo, así como la póliza de multi riesgos para atender eventos de gran impacto en la infraestructura como sismos o incendios, lo cual permite minimizar el riesgo al ocurrir un evento disruptivo, con el fin de que en el menor tiempo posible, se pueda dar continuidad a los servicios que presta la Institución.

De igual forma se asignan recursos para el mantenimiento preventivo y correctivo de instalaciones, plantas eléctricas, sistemas de información, cámaras y accesos físico-lógicos, sistemas de detección temprana y de supresión de incendios, entre otros.



Asimismo, se cuenta con un contrato de seguridad y vigilancia para el resguardo de las instalaciones y activos, y un contrato de servicios de carpintería, albañilería y fontanería, que incluye la atención de emergencias o asuntos urgentes por daños a las instalaciones.

La Institución realiza también, grandes inversiones en Licenciamiento, lo cual incluye antivirus, mecanismos de seguridad para los sistemas y prevención de ataques cibernéticos. Es importante indicar que las estimaciones presupuestarias que se definan en los rubros antes mencionados van a depender en primera instancia del límite presupuestario asignado por el Ministerio de Hacienda y de las necesidades Institucionales que requieran los recursos financieros limitados.

### **J.2. Estimaciones de riesgo de los proyectos**

El Ministerio de Planificación Nacional y Política Económica, MIDEPLAN, es el ente rector en materia de proyectos y es el que define los lineamientos, metodologías y directrices que son de acatamiento para el sector público, en ese contexto, el Registro Nacional identifica los proyectos de inversión a los cuales se les asignan recursos presupuestarios cada año y los registra en el banco de proyectos de este Ministerio.

Existe una metodología específica definida por MIDEPLAN, para la identificación de riesgos en los proyectos de inversión pública, la cual es utilizada por el Registro Nacional para documentar y dar seguimiento a los riesgos identificados en los proyectos.

### **J.3. Valoración de la afectación de ingresos por variables**

Los ingresos que recauda el Registro Nacional se ven afectados directamente por variables macroeconómicas, ya que la aceleración o desaceleración de la economía del país influye en la cantidad de servicios que se demandan (inscripciones, traspasos, compraventa de bienes, entre otros).



Con la entrada en vigor de la Ley 9524, todos los ingresos recibidos por el Registro Nacional son trasladados al Ministerio de Hacienda y a su vez es este ministerio el que asigna y traslada el presupuesto de gastos para la institución, por lo que la variación de ingresos no afecta la asignación de los recursos que se ejecutan.

Sin embargo, se mantiene un registro de los ingresos recaudados, así como una vigilancia continua, que permite informar a los jerarcas sobre situaciones que puedan afectar el servicio que se brinda.

De igual forma, el Departamento Financiero cuenta con un modelo de costos que permite realizar estudios específicos de costo-beneficio para la toma de decisiones o, asignar con base en el principio de servicio al costo, las tarifas anuales basadas en el análisis de gastos y del comportamiento de la demanda de los servicios.

#### **J.4. Control de gasto corriente**

A partir del año 2021, con la implementación de la Ley 9524, el Registro Nacional forma parte del Presupuesto Nacional, por lo que el Ministerio de Hacienda realiza la asignación presupuestaria, estableciendo un límite de gasto anual para los títulos presupuestarios que conforman la Administración Central, con base en lo dispuesto en la Ley 9635, Fortalecimiento de las finanzas públicas, así como en la Ley 8131, Administración Financiera de la República y Presupuestos Públicos.

Por esta razón, el presupuesto del Registro Nacional se encuentra sujeto a la regla fiscal, la cual limita el crecimiento del gasto corriente. Con la aplicación de las políticas para el fortalecimiento de las finanzas públicas y control del gasto, se incrementa la necesidad de definir prioridades para la asignación de recursos que permitan dar continuidad a la prestación de servicios del Registro Nacional.



### **J.5. Análisis de prioridades de recursos**

Bajo el principio de anualidad del Presupuesto, todos los años se realiza el proceso de formulación presupuestaria, mediante el cual cada Dirección del Registro Nacional remite sus necesidades de recursos para el periodo siguiente. Estas necesidades son presentadas ante la Dirección General y la Junta Administrativa para su revisión y aprobación. Como parte del proceso de revisión, se priorizan necesidades y se modifican o excluyen los montos incorporados al anteproyecto de presupuesto, con el fin de ajustarse al límite máximo de gasto que se establece por parte del Ministerio de Justicia para todos sus programas, donde el Registro Nacional constituye el programa 794.

En este proceso de revisión privan los criterios de razonabilidad y eficiencia, dando prioridad al pago de salarios y a los gastos relacionados con garantizar la prestación continua de los servicios del Registro Nacional, tales como servicios básicos, seguros, licencias y mantenimientos de la infraestructura física y tecnológica.

### **J.6. Análisis del impacto financiero-contable que eventualmente podría generar un incidente disruptivo**

El Registro Nacional cumple con los lineamientos establecidos por la Contabilidad Nacional y las Normas Internacionales de Contabilidad del Sector Público (NICSP) para reflejar en los Estados Financieros toda la información contable de forma transparente y oportuna.

Ante un incidente disruptivo se cuenta con la estructura administrativa requerida para realizar el análisis del impacto del evento a nivel financiero para la Institución, a través del Departamento Financiero y sus subprocesos, tales como Contabilidad y Costos y Tarifas.



## **K. Mecanismos de información y comunicación**

La información que se genere en el tema de Continuidad de los servicios y que tenga que ser comunicada a las diferentes partes involucradas, será gestionada por el Departamento de Proyección Institucional, tomando en consideración tres momentos: antes, durante, y después de materializarse un evento.

Para tales efectos el Departamento de cita, dispondrá de un Plan de Comunicación, el cual sensibilizará a los funcionarios sobre el tema de Continuidad de los servicios, indicará las pautas a seguir en caso de materializarse un evento disruptivo y posteriormente comunicará los resultados o lecciones aprendidas que se obtiene una vez realizados los simulacros o materializado el evento disruptivo.

El Plan de comunicación puede ser consultado en la Unidad de Desarrollo Estratégico Institucional.

## **L. Pruebas**

Los simulacros al plan de Continuidad se realizarán una vez al año, como resultado de los estos, se deberán documentar los hallazgos encontrados, los cuales permitirán potenciar las acciones futuras que mitiguen los riesgos ante la materialización de un evento disruptivo, para tales efectos se aplicaron en el 2024 una primera etapa donde se definieron una serie de escenarios posibles donde puede darse una afectación según se detalla a continuación:



### Tabla 13

Tabla de escenarios por servicio crítico para la realización de simulacros

<b>Servicio crítico</b>	<b>Escenario elegido</b>
Mantener disponibles los servicios de placas de manera presencial	Que falle la máquina APP
Mantener disponibles los servicios de placas en el portal web	Que no se tenga acceso al enlace con el Ministerio de Hacienda y el Banco Central con el sistema de PJ
Mantener disponibles las consultas y certificaciones de manera presencial	Que fallen las impresoras
Mantener disponibles las consultas y certificaciones en el portal web	Que no se tenga acceso al SPJ
Recepción, anotación, entrega y notificación de documentos digitales (Ventanilla digital y WIPO-file)	Que no se tenga acceso al SIBIMU
Recibir, asignar citas de presentación, digitalizar, anotar, realizar el reparto, entregar y notificar los documentos físicos de BI, BM, PJ y PI.	Que falle la ventanilla digital
Recibir los documentos físicos calificados de los registradores (digitalizar, archivar y entregar/ notificar los documentos)	Que falle el SIRE (Sistema de Registro Inmobiliario)
Traslado de documentos y placas a las diferentes Regionales	No disponer de la empresa contratada para el traslado. (Correos de Costa Rica)

**Nota:** Elaboración UDEI

### M. Documentación y lecciones aprendidas

En caso de materializarse un evento disruptivo, o después de realizarse las pruebas o simulacros, la Unidad de Desarrollo Estratégico procederá con el levantamiento de la información, con el fin de detectar las incidencias, consecuencias y lecciones aprendidas



durante la gestión para la recuperación de los servicios críticos, estas últimas, serán un insumo fundamental para mejorar el sistema de gestión de la continuidad fortaleciendo el desarrollo de acciones para futuros incidentes disruptivos.

#### **N. Compromiso institucional**

El Registro Nacional se compromete a mantener la continuidad de los servicios críticos definidos como prioritarios, ante eventos disruptivos que pongan en riesgo el desarrollo de las funciones para la prestación de los servicios esenciales, mediante la implementación gradual de acciones que permitan la protección de la vida humana, minimizar los impactos en la gestión, y resguardar los activos institucionales.

#### **O. Seguimiento**

En aras de las mejora continua en materia de Continuidad de los servicios, se realizará un seguimiento anual al Plan de Continuidad , para verificar que la información contenida en este documento se mantenga actualizada y acorde con el alcance establecido y el cumplimiento de los objetivos planteados.