Plan de Recuperación de Desastres

Unidad de Desarrollo Estratégico Institucional

Agosto, 2025

Plan de Recuperación de Desastres

Unidad de Desarrollo Estratégico Institucional

Elaborado por		
Nombre	**Cargo**	**Firma**
Paola Chavarría Agüero	Analista de Fortalecimiento Institutional	PAOLA CHAVARRIA AGUERO (FIRMA) Firmado digitalmente por PAOLA CHAVARRIA AGUERO (FIRMA) Fecha: 2025.08.22 16:18:00 -06'00'
Revisado por		
Adelita Abarca Ortega	Jefe Unidad de Desarrollo Estratégico Institucional	ADELITA ABARCA ORTEGA (FIRMA) Firmado digitalmente por ADELITA ABARCA ORTEGA (FIRMA) Fecha: 2025.08.22 16:29:55 -06'00'
Marcela Coto Garrido	Coordinadora a.i Subproceso Fortalecimiento Institucional	MARCELA COTO GARRIDO (FIRMA) Firmado digitalmente por MARCELA COTO GARRIDO (FIRMA) Fecha: 2025.08.22 16:08:32 -06'00'
Aprobado por		
Agustín Meléndez García	Director General	AGUSTIN MELENDEZ GARCIA (FIRMA) Firmado digitalmente por AGUSTIN MELENDEZ GARCIA (FIRMA) Fecha: 2025.08.25 12:36:33 -06'00'
Agosto, 2025		

TABLA DE CONTENIDO

PRESENTACIÓN

El Plan de Recuperación de Desastres (PRD) que se presenta, forma parte de una estrategia institucional que debe seguir el Registro Nacional, para recuperar sus servicios críticos en un plazo mínimo, después de materializarse un evento disruptivo, como fallas técnicas, ciberataques, desastres naturales, entre otros.

El Registro Nacional, reconoce la importancia de garantizar la continuidad de sus servicios ante cualquier situación que afecta su operación diría, en virtud de su función, la recuperación y disponibilidad de los servicios, se constituye en una prioridad institucional.

Este plan ha sido desarrollado, tomando en consideración los aspectos definidos en la INTE G130:2022/Cor 1:2023, así como la normativa vigente en la materia y de gestión de riesgos, por lo cual se constituye en una herramienta que será revisada periódicamente a fin de incorporar las mejoras que correspondan de acuerdo con la experiencia que para tales efectos se desarrolle.

Es importante mencionar que este plan, responde al requerimiento expreso en el Informe de Auditoría de Carácter Especial sobre la Seguridad de la Información de la Junta Administrativa del Registro Nacional (JARN) 2024, de la Contraloría General de la República, en la recomendación 4.6, la cual indica lo siguiente:

> Elaborar, formalizar, divulgar e implementar el Sistema de Gestión de la Continuidad del Negocio, que contemple e integre al menos: a) la política de continuidad de negocio en la cual se defina el alcance y los objetivos de continuidad del negocio en la institución, b) el plan de continuidad de negocio (BCP) con sus respectivos escenarios, c) el plan de recuperación de desastres (DRP) en atención a los escenarios que surgen del análisis de riesgos de seguridad, d) el análisis de impacto de negocio (BIA), con la estrategia de

respaldo y recuperación, y calendario de pruebas e) objetivos, f) alcance, g) roles y responsabilidades de las partes interesadas, h) pruebas al modelo de continuidad de negocio. i) estrategia de respaldo y recuperación en concordancia con BIA que incluya el calendario de pruebas.

La participación de las personas funcionarias involucradas es clave en los resultados de este plan, y refleja el compromiso institucional con la excelencia, la prevención y la continuidad del servicio público, por lo que; disponer de este documento facilita a la organización contar con una orientación del accionar ante la presencia de eventos disruptivos.

En forma general, el presente PRD retoma aspectos analizados en el Plan de Continuidad aprobado para el Registro Nacional, el documento de Análisis de Impacto del Negocio (BIA), y el documento de Riesgos, que tienen como propósito atender la necesidad de restaurar los servicios críticos después de un evento disruptivo.

Finalmente, es importante mencionar que el documento se encuentra dividido en dos capítulos, el primero hace referencia a los aspectos básicos necesarios a considerar en la elaboración de este documento, el segundo capítulo está relacionado con el desarrollo propiamente de lo que es el Plan de Recuperación Desastres en el Registro Nacional.

CAPÍTULO 1. ASPECTOS GENERALES

A. Propósito

El PRD tiene como propósito definir los elementos necesarios para recuperar la prestación de los servicios críticos del Registro Nacional, y restablecer la operación en el menor tiempo posible para garantizar la continuidad operativa institucional.

B. Alcance

El presente plan considera los aspectos esenciales trabajados hasta el momento, a fin de recuperar los servicios críticos prioritarios definidos para la institución.

C. Objetivos

Objetivo general

Establecer un conjunto de acciones que garanticen la continuidad de los servicios críticos del Registro Nacional ante la presencia de eventos disruptivos, para minimizar pérdidas y restaurar los servicios en el menor tiempo posible.

Objetivos específicos

- Determinar aspectos fundamentales para la recuperación de los servicios críticos.
- Definir los escenarios posibles que surjan del análisis de riesgos.
- Determinar las acciones para dar respuesta ante eventos disruptivos con responsabilidades definidas.

- Desarrollar la sensibilización necesaria a las personas funcionarias del Registro Nacional para estar preparados ante la presencia de eventos disruptivos.
- Desarrollar simulacros o pruebas para actuar eficazmente en situaciones disruptivas.

D. Marco jurídico

El presente marco jurídico, constituye la base normativa que respalda la elaboración, implementación y ejecución del Plan de Recuperación de Desastres del Registro Nacional. Este apartado presenta el sustento legal que orienta la ejecución de acciones frente a la ocurrencia de eventos disruptivos.

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

- 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.
- Norma técnica de Costa Rica (INTECO) denominada INTE/ISO 22301:2015 Seguridad de la sociedad. Sistemas de gestión de continuidad del negocio. Requisitos.
- Formulario para el Seguimiento de la Gestión para la Continuidad de los Servicios Públicos críticos ante la emergencia sanitaria: Formulario Eje N° 1 Gestión de la Continuidad Institucional. Contraloría General de la República.
- Normas técnicas para la gestión y el control de las Tecnologías de información, Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones, 2022.

E. Glosario

El glosario que se detallará a continuación se realiza en aras de bridar una referencia clara y precisa de los términos técnicos, a considerar en el presente documento, estableciendo un lenguaje común que facilite la comprensión e implementación efectiva de los conceptos aquí descritos.

- **Plan de recuperación**: Un plan de recuperación de desastres es un conjunto de estrategias, procedimientos y protocolos que ayudan a las instituciones a recuperar sus servicios ante un evento disruptivo.
- **RTO**: Período de tiempo después de un incidente disruptivo en el que: el servicio debe ser reanudado, o la actividad debe reanudarse, o los recursos deben ser recuperados.
- **RPO**: Punto en el cual la información, requerida por un servicio crítico, puede ser restaurada para permitir la recuperación del servicio.
- **MTPOD**: El tiempo que tomaría para empezar a percibir los efectos adversos que pudieran ocurrir como resultado de no proporcionar un servicio crítico.
- **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.
- **Recuperación:** La implementación gradual de las acciones definidas para volver a la normalidad en la prestación de los servicios.
- **Servicios críticos:** Son aquellos que su entrega tiene una afectación o impacto directo en las partes interesadas considerados como prioritarios.

CAPÍTULO 2. DESARROLLO

En el entorno institucional, se torna necesario la preparación ante eventos disruptivos, estableciendo los mecanismos que aseguren la disponibilidad, integridad y confidencialidad de los servicios críticos definidos.

En este capítulo se presenta el Plan de Recuperación de Desastres (PRD) para el Registro Nacional, como parte de su estrategia de continuidad de los servicios, a fin de establecer las premisas, responsabilidades, procedimientos y recursos necesarios para responder ante incidentes que puedan comprometer los sistemas críticos de la Institución, facilitando la recuperación en la prestación de los servicios.

La elaboración de este plan se fundamenta en el análisis de los servicios críticos definidos, determinando las acciones que correspondan para la recuperación de los servicios en los plazos establecidos en la herramienta del BIA.

A. Premisas

Las siguientes premisas, establecen los supuestos que guiarán la recuperación de las operaciones del Registro Nacional tras un evento disruptivo, asegurando la continuidad del servicio y la protección de la información tal como se muestra a continuación:

- La plataforma tecnológica soporta los sistemas de los servicios identificados como críticos.
- Se dispone de la infraestructura y recursos que soportan la recuperación para los sistemas críticos.
- El responsable de la activación de este Plan es el Director General del Registro Nacional.
- Se realizarán los ajustes que correspondan una vez realizadas las pruebas a los planes correspondientes.
- Se realiza respaldo de la información contenida en las bases de datos.

- Los tiempos relacionados con el RTO, RPO, y MTPOD, corresponde a horas hábiles.

B. Responsabilidades

De acuerdo con la ISO INTE G130:2022/Cor 1:2023, en el apartado 8.4.2.1), el plan de recuperación debe incluir una estructuración de equipos responsables para responder ante la presencia de eventos disruptivos, específicamente se indica lo siguiente:

> la organización pública y sin fines de lucro debe implementar y mantener una estructura, identificando uno o más equipos responsables de responder a las disrupciones. 8.4.2.2) Las funciones y responsabilidades de cada equipo y las relaciones entre los equipos deben ser claramente establecidas.

A continuación, se presenta la tabla de responsabilidades según el cargo en caso de materializarse un evento disruptivo:

Tabla 1

Responsabilidades del cargo

Cargo	Responsabilidades
Director General del RN	Activación del plan.
Director de la Dirección de Informática	Recuperación de datos y sistemas.
Directora de la Dirección de Servicios	Coordinación de las acciones a realizar para la recuperación de los servicios críticos.
Jefatura de Proyección Institucional	Manejo de comunicaciones internas y externas.
Coordinadora Subproceso de Fortalecimiento de la Unidad de Desarrollo Estratégico Institucional	Dar seguimiento al cumplimiento de las acciones y procedimientos establecidos.

Nota: Elaboración UDEI

C. Mecanismos de recuperación

Tal como lo menciona la INTE/ISO 22313:2015, apartado 8.4.5, relacionado con la recuperación de los servicios, es importante considerar los procedimientos establecidos para restituir la continuidad de las operaciones definidas como críticas.

Estos procedimientos fueron definidos por la Dirección de Servicios para cada uno de los servicios críticos, con el propósito de atender algún evento disruptivo, tal como se indica en la tabla 2:

Tabla 2

Procedimientos según servicio crítico

Servicio crítico	Procedimiento para atender el servicio crítico
Mantener disponibles los servicios de placas de manera presencial	DSE-PSE-023: Recuperación del servicio de placas ante un evento disruptivo.
Mantener disponibles los servicios de placas en el portal web	DSE-PSE-023: Recuperación del servicio de placas ante un evento disruptivo.
Mantener disponibles las consultas y certificaciones en el portal web	DSE-PSE-024: Recuperación del servicio de consultas y certificaciones ante un evento disruptivo.
Mantener disponibles las consultas y certificaciones de manera presencial.	DSE-PSE-024: Recuperación del servicio de consultas y certificaciones ante un evento disruptivo.
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.
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.

Servicio crítico	Procedimiento para atender el servicio crítico
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.
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: Procedimientos elaborados con la Dirección de Servicios.

Tomando en consideración tanto los servicios críticos como los procedimientos mostrados en la tabla anterior, es importante mencionar que la Dirección de Informática tiene documentado un Plan de Recuperación de TI, que establece los mecanismos de recuperación, tal como se muestra en la siguiente tabla:

Tabla 3

Mecanismos de recuperación de la Dirección de Informática

Servicio crítico	Riesgo	Sistemas críticos	RPO	RTO	MTPOD	Como lo atiende la DIR	Está documentada	Riesgos de TI
Mantener disponibles los servicios de placas de manera presencial	**Riesgo: 279** Caída en el sistema Sipla	Sistemas SIBIMU, SIPLA, E-POWER, SPJ y los webservice (COSEVI, DNN, INS, Registro Civil).	1	16	20	En este caso la DIN únicamente puede brindar acompañamiento a la Dirección de Servicios porque esa dirección gestiona ese proveedor. La DIN atiende las solicitudes técnicas que el proveedor indique y corresponda realizar.	Plan de respuesta ante desastres (DRP) de los servicios críticos de TI	Este escenario está en la gestión de riesgos de la Dirección de Servicios
Mantener disponibles los servicios de placas en el portal web	**Riesgo 264**: Interrupción del servicio de consultas, certificaciones y placas en el portal web.	Portal Institucional, SIBIMU, SIPLA, E-POWER, SISTEMA DE PAGOS DEL BCR, SPJ y los webservice (COSEVI, DNN,	1	16	20	Se aplica una guía para verificar cuentas externas y un protocolo para la atención de incidentes.	Plan de respuesta ante desastres (DRP) de los servicios críticos de TI	Riesgos Nº 9, Incidentes y problemas en la prestación de servicios de TI.

Servicio crítico	Riesgo	Sistemas críticos	RPO	RTO	MTPOD	Como lo atiende la DIR	Está documentada	Riesgos de TI
		INS, Registro Civil).						
Mantener disponibles las consultas y certificaciones en el portal web	**Riesgo 264**: Interrupción del servicio de consultas, certificaciones y placas en el portal web.	Portal Institucional, SIBIMU, SPJ, SIRE, SIRI, SIP, IPAS, SEC, SIPLA, E-POWER, SISTEMA DE PAGOS DEL BCR.	1	16	20	Se aplica el protocolo para la atención de incidentes.	Plan de respuesta ante desastres (DRP) de los servicios críticos de TI	Riesgos Nº 9, Incidentes y problemas en la prestación de servicios de TI.
Mantener disponibles las consultas y certificaciones de manera presencial.	**Riesgo 283**: Imposibilidad de atención de consultas y emisión de certificaciones físicas.	Se requiere de los sistemas sustantivos de todos los Registros.	1	24	20	Aplica el procedimiento para la gestión de casos del Departamento Servicio al Usuario de TI y el protocolo para la atención de incidentes.	Plan de respuesta ante desastres (DRP) de los servicios críticos de TI	Riesgos Nº 9, Incidentes y problemas en la prestación de servicios de TI.
Recepción, anotación, entrega y notificación de documentos digitales (Ventanilla digital y WIPO-file).	**Riesgo 268:** Interrupción del servicio de recepción, anotación, entrega y notificación de documentos digitales (ventanilla digital y WIPO file).	digital, WIPO File, SIDU, SIRE, SPJ, SIBIMU, SIP, IPAS, componente de firma digital, web services: DNN, Registro Civil.	1	24	32	Se aplica el protocolo para la atención de incidentes.	Plan de respuesta ante desastres (DRP) de los servicios críticos de TI	Riesgos Nº 9, Incidentes y problemas en la prestación de servicios de TI.

Servicio crítico	Riesgo	Sistemas críticos	RPO	RTO	MTPOD	Como lo atiende la DIR	Está documentada	Riesgos de TI
Recibir, asignar citas de presentación, digitalizar, anotar, realizar el reparto, entregar y notificar los documentos físicos de BI, BM, PJ, y PI.	**Riesgo 269**: interrupción del servicio de recepción, anotación, entrega y notificación de documentos físicos.	SIDU, SIRE, SPJ, SIBIMU, SIP, IPAS, E- POWER, E-SCAN.	1	24	32	Se aplica el protocolo para la atención de incidentes.	Plan de respuesta ante desastres (DRP) de los servicios críticos de TI	Riesgos Nº 9, Incidentes y problemas en la prestación de servicios de TI.
Recibir los documentos calificados de los registradores (digitalizar, archivar y entregar/notificar los documentos).		SIRE, SPJ, SIBIMU, SIP, IPAS, E- POWER, E-SCAN.	1	24	32	Se aplica el protocolo para la atención de incidentes.	Plan de respuesta ante desastres (DRP) de los servicios críticos de TI	Riesgos Nº 9, Incidentes y problemas en la prestación de servicios de TI.
Traslado de documentos y placas a las diferentes Regionales.	**Riesgo 280**: No disponer de la contratación para el traslado de documentos. **Riesgo 281**: Caídas de los sistemas.	SIRE, SPJ, SIBIMU, SIP, E-POWER, E-SCAN.	1	24	32	No aplica a la Dirección de Informática gestionar problemas de disponibilidad de servicios de Correos de Costa Rica		

D. Análisis de riesgos de Servicios Críticos

Para el análisis de riesgos en primera instancia se realizó una sesión con la Dirección de Servicios, posteriormente se analizaron los riesgos definidos por esta, con la Dirección de Informática, donde se determinó la necesidad de incorporar dentro de las causas de los riesgos a los servicios críticos, la información

Tabla 4

Análisis de la causa ataques de ciberseguridad

Riesgo	Causa	Medidas	Indicador	Meta	Evidencia del cumplimiento	Efecto de la medida
264: Interrupción del servicio de consultas, certificaciones y placas en el portal web.	Ataques de ciberseguridad	Soluciones de seguridad de la información	Porcentaje de disponibilidad de las herramientas	98%	Se dispone de las herramientas actualizadas y son efectivas y además se cuentan con un indicador de disponibilidad de los sistemas de seguridad. El resultado es 100% a junio 2025.	Apoyar la implementación de controles para prevenir posibles incidentes de seguridad
268: Interrupción del servicio de recepción, anotación, entrega y notificación de documentos digitales (ventanilla digital y WIPO-File).		Segmentación de infraestructura tecnológica.	% de cobertura de segmentación	100%	Configuraciones de los equipos. Documentación técnica de las gestiones de las redes	Permitir únicamente los accesos autorizados a la red

Riesgo	Causa	Medidas	Indicador	Meta	Evidencia del cumplimiento	Efecto de la medida
269: Interrupción del servicio de recepción, anotación, entrega y notificación de documentos físicos.	Ataques de ciberseguridad	Se dispone de mecanismos de control de acceso a la red	% de cobertura de control de acceso a la red alámbrica	100%	´-Configuraciones de los equipos - Documentación técnica de las gestiones de las redes	Permitir únicamente los accesos autorizados a la red
279: Caída del sistema SIPLA		Mecanismos de alta disponibilidad	% de recursos críticos cubiertos con mecanismos de alta disponibilidad.	93%	96,74% de recursos críticos según matriz a marzo 2025.	Minimizar los efectos de la falla en un componente de la plataforma tecnológica
281: Caídas de los sistemas		Respaldos de la información	Porcentaje de efectividad en la toma de respaldos	95%	Existen diferentes estrategias para realizar los respaldos. De acuerdo con los indicadores del Depto. de Infraestructura Tecnológica se obtiene un 100% de efectividad a junio del 2025.	Evitar la pérdida de información en el caso que haya una falla en la infraestructura
283: Imposibilidad de atención de consultas y emisión de certificaciones físicas.		Se dispone de documentación técnica (ejemplo: guías, protocolos, procedimientos, entre otros).	Porcentaje de documentos revisados	100%	Confección anual del Acta de Revisión, y actualización al 100% de la documentación que corresponda.	Contar con instrucciones de trabajo revisados para atender la interrupción de los servicios

Riesgo	Causa	Medidas	Indicador	Meta	Evidencia del cumplimiento	Efecto de la medida
	Ataques de ciberseguridad	Programa de concienciación al personal en temas de ciberseguridad	Campaña anual de concienciación ejecutada	1	Se coordina con Proyección Institucional para el envío de la campaña.	Fortalecer los conocimientos de seguridad en los funcionarios de la Institución
		Actualización periódica de plataforma tecnológica.	Informe anual sobre el desempeño de la plataforma tecnológica del departamento respectivo.	2	Documento presentado	Evitar la obsolescencia de la plataforma tecnológica

Nota: Elaboración UDEI con participación de la Dirección de Informática

E. Sensibilización

La continuidad de los servicios requiere de una oportuna sensibilización a fin de fomentar la cultura organizacional enfocada en el conocimiento, la prevención, y preparación para la recuperación ante eventos disruptivos que puedan afectar la operación normal de la Institución y por ende su imagen.

En ese sentido, la sensibilización tiene como propósito concientizar a las personas funcionarias del Registro Nacional, sobre la importancia de disponer de un Plan de Recuperación Desastres (PRD), destacando el papel que cada funcionario involucrado juega en su ejecución, fortaleciendo el compromiso institucional que garantice la respuesta oportuna y coordinada frente a la presencia de la materialización de un evento disruptivo.

La implementación exitosa de este Plan requiere de la ejecución no solo de los procedimientos establecidos, sino también del entendimiento y la participación de las personas colaboradoras involucradas.

F. Acciones para la recuperación de los servicios críticos

La recuperación oportuna de los servicios críticos es uno de los aspectos fundamentales de este Plan, en ese sentido es necesario tener presente las acciones que se han desarrollado en distintos temas tales como: Procedimientos, Riesgos, y Plan de Recuperación de TI, para restablecer de manera oportuna los servicios esenciales que la Institución ha definido ante la presencia de un evento disruptivo.

En caso de materializarse un evento disruptivo, además de tomar en cuenta los temas mencionados anteriormente, se debe considerar la ejecución de acciones tales como:

- Evaluación de los daños que genera el evento disruptivo.

- Activación del Plan de Recuperación de Desastres aplicando los procedimientos y medidas ya establecidas.
- Comunicación a las partes involucradas en la interrupción de los servicios críticos.
- Activación de Plan de Recuperación de Tecnología de la Información.
- Reanudación de los servicios de acuerdo con las prioridades definidas por el jerarca.

ANEXO

Plan de respuesta ante desastres (DRP) de los servicios críticos de la Dirección de Informática.