Pl

Plan de Continuidad del Sistema Digital Unificado (SICOP)

Dirección de Contratación Pública.
Departamento de Compra Pública Estratégica
Unidad de Gestión del Sistema Digital Unificado
Julio, 2025
Versión 01

MINISTERIO DE HACIENDA | GOBIERNO DE COSTA RICA

1 Tabla de contenido

1. Generalidades

1.1 Introducción

El presente documento constituye el Plan de Continuidad del Sistema Digital Unificado (SICOP), elaborado en cumplimiento de la disposición emitida por la Contraloría General de la República, conforme a lo establecido en los párrafos 2.20 al 2.31 del informe de fiscalización DFOE-FIP-IAD-00003-2024. Su propósito es garantizar la operación continua, segura, resiliente y eficaz del sistema que soporta los procesos de contratación pública a nivel nacional.

Este plan ha sido desarrollado por la Unidad de Gestión del Sistema Digital Unificado (UGSDU) de la Dirección de Contratación Pública (DCoP), y revisado por la Dirección de Planificación Institucional del Ministerio de Hacienda. En su formulación se ha aplicado un enfoque integral y preventivo, alineado con los principios y requisitos establecidos en la norma internacional ISO 22301:2019, referente a los sistemas de gestión de continuidad del negocio, y la norma ISO 31000 sobre gestión de riesgos.

Asimismo, incorpora herramientas institucionales como el Sistema de Valoración de Riesgos Institucionales (SEVRI), el Plan de Continuidad de Negocio del Ministerio de Hacienda, el Plan de contingencia del Servicio SICOP y el Análisis de Impacto del Negocio (BIA) para el SDU, lo que permite establecer medidas claras para responder ante interrupciones, recuperar operaciones críticas, y restaurar la funcionalidad plena del sistema en tiempos aceptables.

Este plan tiene como finalidad verificar y asegurar la activación oportuna de mecanismos de continuidad la identificación de etapas críticas del proceso transaccional, así como la recuperación íntegra y segura de los datos afectados durante la interrupción. Asimismo, contempla la evaluación periódica de su efectividad y la mejora

continua del plan, con el fin de fortalecer la resiliencia institucional y preservar la integridad, disponibilidad y confidencialidad de la información gestionada por el sistema.

1.2 Objetivo

Establecer un marco estratégico y operativo que garantice la continuidad del funcionamiento del Sistema Digital Unificado (SICOP), ante la ocurrencia de eventos disruptivos o catastróficos que puedan comprometer la prestación del servicio de contratación pública en el Estado costarricense.

1.3 Alcance

Aplica para el Sistema Digital Unificado (SDU), la Dirección de Contratación Pública, Racsa, como prestador del servicio del SDU y a todos los usuarios del sistema y las instituciones que representan, además de los proveedores registrados.

1.4 Documento Referencia

Los documentos a los cuales se debe hacer referencia para mantener este Plan de Continuidad de Negocio se muestran en la siguiente tabla:

Documento	Última Actualización
1. MH-DIPI-PR002-POL-06 Política para la Continuidad del Negocio	
2. MH-DIPI-PR002-POL-002 Política del Sistema de Valoración de Riesgo Institucional.	

3. Plan de Continuidad de Negocio Ministerio de Hacienda	Octubre 2024
4. "Plan de Contingencia Tecnológica Sistema Integrado de Compras Públicas SICOP". 5.	Febrero 2025
6. MH-DIPI-PRO02-FOR-019 Herramienta SEVRI_SDU	Enero 2025
7. MH-DIPI-PRO02-FOR-021 Formulario Análisis de Impacto del Negocio-SDU	Junio 2025

2. Plan de Continuidad de Negocio

2.1 Evaluación de los riesgos y análisis del impacto al negocio

Con fundamento en los resultados obtenidos de la aplicación del instrumento institucional MH-DIPI-PRO02-FOR-021, se determinó que el proceso de Gestión del Sistema Digital Unificado (SDU) presenta un impacto total de 2,80, lo cual corresponde a una clasificación de criticidad media, conforme a la escala de valoración establecida por la institución. Este nivel de criticidad refleja impactos que oscilan entre moderados y altos en variables estratégicas tales como el cliente externo (4,00), la imagen corporativa (3,00), el cumplimiento del marco legal y regulatorio (3,00) y el cliente interno (3,00). Cabe señalar que el impacto financiero (1,00) se identifica como el de menor relevancia dentro del análisis efectuado.

En concordancia con estos resultados, se ha establecido un Tiempo Objetivo de Recuperación (RTO) superior a un día e inferior o igual a dos días, así como un Máximo Tiempo Tolerable de Disrupción (MTPD) que se sitúa entre más de cuatro días y hasta ocho días. Dichos parámetros exigen la existencia de procedimientos formalizados para la activación del plan, la respuesta técnica ante

contingencias, la restauración de la operatividad y la implementación de mecanismos efectivos de comunicación con las partes interesadas clave del sistema.

El análisis anterior reafirma la necesidad de implementar mecanismos de recuperación que sean escalables y sostenibles, acompañados de estrategias de respaldo automatizadas, pruebas periódicas de restauración y una coordinación interinstitucional robusta, particularmente con actores críticos como RACSA y DTIC. Todo lo anterior con el propósito de mitigar el impacto de posibles eventos disruptivos sobre la continuidad del sistema nacional de contratación pública y garantizar su disponibilidad, integridad y confiabilidad ante situaciones adversas.

Resumen del Análisis de Impacto y Riesgos – Sistema Digital Unificado (SDU)

Categoría	Detalle	
Sistema evaluado	Sistema Digital Unificado	
Instrumentos utilizados	Herramienta SEVRI_SDU	Formulario Análisis de Impacto del Negocio-SDU
Impacto Total	2,80 (Criticidad media)	
Variables evaluadas	**Valor del impacto**	**Nivel de riesgo**
Cliente externo	4	Alto
Imagen corporativa	3	Medio
Cumplimiento legal y regulatorio	3	Medio
Cliente interno	3	Medio
Impacto financiero	1	Bajo

Tiempo Objetivo de Recuperación (RTO)	Más de 1 día y hasta 2 días
Máximo Tiempo Tolerable de Disrupción (MTPD)	Más de 4 días y hasta 8 días
Implicaciones clave	Requiere procedimientos documentados de activación, respuesta, restauración y comunicación
Recomendaciones	Implementar mecanismos de recuperación escalables, respaldos automatizados y coordinación con RACSA y OCI

2.2 Sistemas Críticos, Procesos, Activos de información y Personas

La identificación y clasificación de los sistemas críticos, procesos esenciales, activos de información y personas clave constituye un componente central para la planificación de la continuidad operativa del Sistema Digital Unificado (SDU). Esta sección tiene como propósito establecer el inventario y la priorización de los elementos que sostienen las funciones vitales del sistema, considerando su nivel de criticidad, interdependencia y el impacto potencial ante una disrupción. El análisis de estos elementos permite orientar de manera precisa las estrategias de recuperación, asignación de recursos y mecanismos de respuesta ante eventos que comprometan la operatividad del sistema.

El enfoque adoptado se basa en criterios institucionales de evaluación de impacto, tiempos de recuperación aceptables (RTO) y tiempos máximos tolerables de disrupción (MTPD), conforme al modelo de gestión del riesgo adoptado por la organización. Asimismo, se reconocen las interrelaciones entre componentes tecnológicos, procesos funcionales, activos de información y el recurso humano especializado, entendiendo que la resiliencia del SDU depende de una articulación efectiva entre estos factores. La correcta identificación de estos elementos críticos permitirá establecer acciones preventivas, procedimientos de recuperación y planes de respaldo orientados a preservar la continuidad del servicio público de contratación estatal.

2.3 Sistemas Críticos

Los sistemas críticos constituyen la infraestructura tecnológica esencial para la operación continua y segura del Sistema Digital Unificado (SDU). Esta sección tiene como objetivo identificar aquellos sistemas cuya indisponibilidad, interrupción o mal funcionamiento podría generar un impacto significativo en la prestación del servicio, en el cumplimiento normativo o en la integridad de los procesos de contratación pública. La categorización de estos sistemas permite establecer prioridades de recuperación y diseñar estrategias de respaldo y contingencia acordes con su nivel de criticidad.

En este contexto, se consideran sistemas críticos aquellos que sustentan funciones transaccionales, autenticación de usuarios, integridad de datos, trazabilidad documental, interoperabilidad con otras plataformas estatales y disponibilidad de servicios para usuarios internos y externos. La adecuada gestión de estos sistemas implica no solo contar con arquitecturas redundantes y planes de recuperación tecnológica, sino también con esquemas de monitoreo

continuo, pruebas periódicas de contingencia y una clara definición de roles y responsabilidades institucionales.

Sistema(s)	Dirección web o descripción de posible falla	Periodo de tiempo crítico	Respaldo de datos (Ubicación y tiempo de respaldo)
Caída del sistema principal (sitio primario)	https://www.sicop.go.cr/index.jsp	2 hrs/6hrs	Los respaldos del SICOP están alojados en la plataforma Oracle Cloud Infrastructure (OCI) y se dividen en dos niveles: 1. Object Storage de OCI (nube principal) Aquí se almacenan los resguardos automáticos de bases de datos. 2. Sitio de Recuperación ante Desastres (DR) -Ubicado en una región geográfica distinta a la
Fallas en servicios asociados claves	Falla de comunicación entre SINPE – SICOP para validar certificados digitales.	3 hrs	
	Falla de comunicación entre SINPE – SICOP (CGP (Centro Gestor de Pagos).	6 hrs	
Fallas en la interoperabilidad con plataformas clave	Falla de comunicación entre sistemas de CCSS (SICERE) y FODESAF.	6 hrs	
	Falla comunicación Registro Nacional	6 hrs	
	Falla de comunicación entre una Institución Garante – SICOP.	No especifico/Se mide impacto para toma de decisiones	
	Falla de comunicación entre CGR – SICOP (SIAC).	No especifico/Se mide impacto	

		para así tomar de decisiones	del sitio principal. -Mantiene una copia en línea sincronizada de la base de datos, gracias al servicio Oracle Active Data Guard, que permite alta disponibilidad, replicación en tiempo real y recuperación inmediata ante desastres
	Falla de comunicación entre SICOP y SIGAF, https://sigaf.hacienda.go.cr/sap/bc/gui/sap/its/webgui?sap-client=500&sap-language=ES#	No especifico/Se mide impacto para así tomar de decisiones	
Fallos de proveedores tecnológicos	https://ocistatus.oraclecloud.com	2hrs	
Ciberataques o pérdida de datos	NA	Cuando sea detectado	
Cambios regulatorios no implementados	Tardanza del proceso administrativo y en el desarrollo de requerimiento	Fecha de entrada en vigor	
Saturación de usuarios y carga de transacciones	NA	Cuando sea detectada la afectación	

2.4 Procesos y personas críticas

La identificación de procesos y personas críticas es un elemento fundamental en la gestión de la continuidad operativa del Sistema Digital Unificado (SDU), ya que permite reconocer las funciones organizacionales indispensables para la prestación ininterrumpida

del servicio, así como los perfiles humanos cuya experticia y responsabilidad resultan esenciales ante escenarios de disrupción. Esta sección detalla los procesos que, por su naturaleza estratégica o por el alto impacto institucional que conlleva su interrupción.

De igual forma, se identifican las personas críticas, entendidas como aquellos funcionarios o unidades responsables de la operación directa, soporte técnico, gestión funcional, monitoreo de riesgos y toma de decisiones en situaciones de emergencia. La continuidad de estos roles requiere de esquemas de disponibilidad, redundancia operativa, planes de sustitución temporal y protocolos de comunicación claros, de manera que se garantice la resiliencia institucional incluso en condiciones adversas.

Proceso	Personas Crítica/ RACSA	Actividad crítica	Personas Crítica/ DCoP	Actividad Critica
Todos los módulos del SDU	Coordinador General del Área de SICOP	Lidera el Equipo de Coordinación General de Continuidad y Recuperación, que es el único con potestad para autorizar la activación del Plan de Contingencia ante una	Administrador de Contrato, Subdirector (a), Director(a) de DCoP y coordinador de la UGSDU.	Equipo operativo que es el único con potestad para autorizar la activación del Plan de Continuidad ante una falla o desastre y por recomendación de RACSA.
Herramientas de monitoreo y alerta temprana para anomalías en disponibilidad o rendimiento.				
Mesa de Ayuda SICOP				
Validación de servicios asociados e interoperabilidad				
Imposibilidad de Institución o Proveedor de acceso el SDU				

Aplicación de cambios regulatorios no implementados		falla o desastre.		
Pruebas de integridad de los datos restaurados				

3. Plan de Recuperación de Desastres

La creciente dependencia de las tecnologías de información en los procesos de contratación pública impone la necesidad de contar con mecanismos sólidos que garanticen la resiliencia operativa ante eventos disruptivos. En este contexto, el Plan de Recuperación de Desastres constituye un componente esencial del Plan de Continuidad del Sistema Integrado de Compras Públicas (SICOP), orientado a restablecer en el menor tiempo posible los servicios críticos del sistema tras una interrupción mayor, preservando la integridad de los datos y la disponibilidad del servicio.

Esta sección presenta la estrategia y las acciones específicas que deben ejecutarse en caso de que el sitio principal de operación se vea comprometido por una contingencia severa. Incluye los procedimientos de activación del sitio alterno de recuperación, las responsabilidades de los equipos técnicos involucrados, los mecanismos de respaldo y restauración, así como los protocolos de comunicación institucional. La implementación oportuna y coordinada de este plan es fundamental para minimizar el impacto sobre las instituciones usuarias, proveedores y demás actores del ecosistema de contratación pública, asegurando la continuidad de los procesos bajo estándares de confiabilidad, eficiencia y transparencia.

Este plan debe considerar:

1. La infraestructura tecnológica, incluyendo servidores, bases de datos, servicios de almacenamiento, redes, clústeres de procesamiento y mecanismos de respaldo.
2. Los procesos críticos del sistema (recepción de ofertas, firma digital, adjudicación, recursos, pagos, entre otros).
3. La interoperabilidad con sistemas externos como los de la Gestión Financiera, SINPE, CCSS, CGR, Registro Nacional, entre otros.
4. Las instituciones usuarias del SDU, los proveedores y los entes garantes involucrados en los procedimientos de compra.
5. El sitio principal de operación y el sitio alterno de recuperación (Disaster Recovery – DR).
6. La cadena de decisiones operativas y estratégicas liderada por la DCOP en coordinación con la unidad técnica del SDU.

3.1 Estructura de manejo de los incidentes

La detección inicial de un incidente puede originarse a partir de la supervisión técnica continua de la plataforma o mediante reportes de fallos por parte de los usuarios del Sistema Digital Unificado (SDU). La Unidad de Gestión del SDU de la Dirección de Contratación Pública (DCoP) es responsable de canalizar de forma oficial el primer reporte técnico del evento a la Mesa de Ayuda SICOP, activando el protocolo de evaluación descrito en el documento Plan de Contingencia Sistema Integrado de Compra Pública SICOP. Adicionalmente, se habilita la participación de las instituciones usuarias del SDU como actores coadyuvantes, quienes están facultadas para reportar fallos, interrupciones o comportamientos anómalos que puedan comprometer la continuidad operativa.

La notificación debe realizarse a través del canal formal definido por RACSA en el documento Plan de continuidad Sistema Integrado de Compra Pública SICOP:

Correo electrónico: sicop@racsa.go.cr
Teléfono: 800-SICOP-00 (800-74267-00)
Horario de atención: Lunes a domingo, 24/7, con personal técnico capacitado.

Los reportes deben contener como mínimo: descripción del incidente, captura de pantalla (si aplica), fecha y hora estimada, nombre de la persona remitente, unidad administrativa e institución.

La recepción y registro del incidente por parte de la Mesa de Ayuda da inicio al procedimiento formal de evaluación técnica y recuperación, bajo supervisión del equipo de contingencia. Dependiendo del tiempo de afectación y pronósticos de solución entra en funcionamiento este Plan de Continuidad del Negocio.

La Dirección de Contratación Pública (DCOP) es el ente rector responsable de validar y actualizar el presente plan, emitir directrices vinculantes y garantizar la articulación institucional ante escenarios de continuidad. Para ello, se establecen comités y equipos con funciones diferenciadas:

1. Comité Central de Continuidad SDU: presidido por la DCOP, con funciones de supervisión, autorización de activación y seguimiento estratégico. Recae en la figura del Administrador de Contrato, en coordinación con la Dirección y el coordinador de la UGSDU.
2. Equipo de coordinación general de continuidad y recuperación: Es el Grupo en RACSA encargado de autorizar la puesta en ejecución el plan de contingencia y coordinar con DCoP la puesta en marcha del plan de continuidad según sea la efectividad de la atención del evento presentado.
3. Coordinadores Institucionales: enlaces designados por cada institución usuaria, responsables de activar planes de

continuidad locales y mantener comunicación activa con el Comité Central.

3.2 Plan de respuesta ante indisponibilidad prolongada o ciberataque con pérdida de funcionalidad crítica del SDU

Ante la posibilidad de una contingencia severa que imposibilite la restauración o funcionamiento operativo del Sistema Digital Unificado (SDU) —ya sea por un ciberataque dirigido, por daño físico a la infraestructura crítica, por corrupción de datos irrecuperable o por otra causa que genere indisponibilidad prolongada— es imprescindible establecer un protocolo formal de respuesta, basado en principios de continuidad del Estado, legalidad, trazabilidad y minimización de impacto a los procedimientos de contratación pública.

3.3 Declaratoria de Incidente Crítico

La Dirección de Contratación Pública (DCOP), como ente rector, en coordinación con el Coordinador General del Área de SICOP, deberá declarar formalmente el estado de incidente crítico de disponibilidad, mediante resolución administrativa, cuando:

- Se verifique técnicamente que no es posible restablecer el servicio ni parcial ni completamente y se determina un tiempo razonable para la declaración, éste coordinado entre las partes según sea el escenario de afectación.

- Se confirme que uno o más módulos críticos están comprometidos de forma irrecuperable en el corto plazo.

- Se identifique evidencia sustantiva de afectación por ataque cibernético, imposibilitando la confianza operativa del entorno.

Dicha resolución deberá incluir la duración estimada de la contingencia, el alcance funcional afectado, las medidas provisionales autorizadas y el marco de excepción que regirá durante la operación fuera de sistema.

3.4 Activación del Protocolo de Operación Manual Sustituta

Durante el periodo de afectación se implementará un Protocolo de Operación Manual Sustituta (POMS) para garantizar la continuidad mínima de los procesos de contratación. Esta modalidad debe operar bajo estándares controlados de trazabilidad, integridad documental y responsabilidad institucional, y será aplicable únicamente mientras persista la imposibilidad técnica de utilizar el sistema. La DCoP mediante resolución autorizará a las instituciones el uso de protocolo.

3.5 Alcance del Protocolo

Las actividades que podrán ser ejecutadas manualmente y en forma física, previa autorización por resolución de la DCOP, incluyen:

- Desde el inicio del procedimiento de la contratación, que incluye: solicitud de pedido, decisión inicial, elaboración de pliegos de condiciones, invitaciones a los concursos, recepción y tramitación de recursos, recepción y apertura de ofertas, acto final, formalización contractual, emisión de pedidos y cualquier otro que abarque la finalización total del procedimiento.

3.6 Procedimiento Operativo Manual

DCoP:

Emite la resolución de activación del protocolo del plan de continuidad del negocio.
Notifica la resolución de activación del protocolo al jerarca de cada institución pública.

Cada Institución pública deberá:

1. Comunicar la resolución emitida por la DCoP.
2. Organizar a lo interno la implementación del uso del protocolo para garantizar la eficiencia, eficacia y transparencia en los procedimientos de contratación pública que inicien o que deban continuar en forma manual y física.
3. Las Unidades de Compra o Proveedurías Institucionales, serán las responsables de llevar el expediente físico que se llegara a levantar para efectos del inicio de una nueva contratación o continuación del procedimiento de la contratación.
4. Cada expediente deberá llevarse en orden cronológico y foliado.
5. Los documentos físicos que emitan para realizar alguna parte del procedimiento de la contratación deberá contener la misma información que se encuentra en el SICOP, por ejemplo: pliegos de condiciones, ordenes de inicio, ordenes de pedido, resoluciones, entre otros.

3.7 Registro Posterior de Tareas Manuales en el Sistema

La DCoP notificará a las instituciones una vez restablecida la operación total o parcial del SDU y dará el plazo perentorio para el registro de las actuaciones que realizaron fuera del sistema por la activación del protocolo, una vez realizado el registro el jerarca de la institución deberá remitir una declaración jurada a la DCoP el haber cumplido con dicha obligación.

3.8 Carga de información al SDU

- Cada institución deberá designar un **Equipo de Transcripción y Validación**, encargado de digitalizar o registrar en el SDU todos los actos realizados fuera de sistema.
- En el expediente del procedimiento se deberá incluir un documento que identifique que el acto fue llevado a cabo durante el incidente crítico. Como respaldo se pueden incluir las notificaciones realizadas por la DCoP durante el lapso en cuestión.

3.9 Medidas Complementarias y de Prevención

Una vez superado el incidente, se deberán ejecutar acciones adicionales para mitigar futuros riesgos y robustecer la resiliencia del sistema:

- Auditoría forense del incidente (cuando se trate de ciberataque), liderado por RACSA con apoyo de entes especializados como la DTIC.
- Evaluación de fallos de gobernanza, comunicaciones o arquitectura tecnológica.
- Actualización del Plan de Continuidad y de los protocolos de operación manual.
- Capacitación a enlaces institucionales sobre procedimientos de emergencia.

4. Estrategias de recuperación para los riesgos estratégicos identificados.

Riesgo	Cliente externo		
Probabilidad	Alta	Impacto	4

Estrategia de recuperación	Establecer canales alternos de atención al usuario (correo institucional, líneas telefónicas y formularios manuales). Implementar una mesa de ayuda temporal y brindar instructivos de procedimientos manuales. Una vez restablecido el sistema, capturar en el sistema todas las transacciones ejecutadas manualmente.

Riesgo	Imagen corporativa		
Probabilidad	Media	Impacto	3
Estrategia de recuperación	Activar plan de comunicación institucional ante incidentes para informar con transparencia, oportunidad y claridad. Publicar comunicados oficiales sobre las acciones correctivas y tiempos estimados de restauración. Demostrar control y respuesta organizada para mitigar daños reputacionales.		

Riesgo	Cumplimiento legal y regulatorio		
Probabilidad	Medio	Impacto	3
Estrategia de recuperación	Implementar registros manuales con respaldo legal para mantener la trazabilidad y garantizar cumplimiento normativo. Establecer mecanismos alternos de validación documental y asegurar firmas responsables. Coordinar con entes reguladores para formalizar los procedimientos temporales adoptados.		

Riesgo	Cliente Interno

Probabilidad	Medio	Impacto	3
Estrategia de recuperación	Activar procedimientos de continuidad operativa con roles definidos y capacitación previa al personal crítico. Facilitar herramientas ofimáticas y medios físicos/digitales de respaldo para garantizar la operación. Monitorear la carga de trabajo manual y establecer prioridades para minimizar el impacto interno.		

Riesgo	Impacto financiero		
Probabilidad	Bajo	Impacto	1
Estrategia de recuperación	Realizar control paralelo manual de las órdenes de compra, pagos y transacciones presupuestarias. Validar con respaldo contable y financiero todas las operaciones realizadas durante el incidente. Incluir auditorías post-evento para evaluar afectación y tomar acciones correctivas si aplica.		

5. Mantenimiento del Plan de Continuidad

5.1 Pruebas y revisión periódica del PCN

La revisión del Plan de continuidad de Negocio se debe efectuar anualmente, según lo dispuesto en MH-DIPI-PRO02-POL-006 Política Continuidad del Negocio y el diseño de las pruebas está sujeta al Plan de Continuidad de Negocio Institucional del Ministerio de Hacienda.

5.2 Descripción de las pruebas

En el marco de la gestión integral de la continuidad operativa, la ejecución periódica de pruebas constituye un componente esencial para validar la eficacia del Plan de Continuidad del Sistema. Estas pruebas permiten verificar, en condiciones controladas o simuladas, la capacidad institucional para responder de forma oportuna y

coordinada ante eventos disruptivos que comprometan la operación normal del sistema transaccional. Además, brindan la oportunidad de familiarizar a los actores clave con sus funciones, evaluar la pertinencia de los procedimientos establecidos y detectar posibles debilidades u omisiones en el diseño del plan.

La realización estructurada de pruebas facilita no sólo el fortalecimiento técnico y organizacional, sino también el cumplimiento de principios de mejora continua y resiliencia institucional. Por medio de estas actividades, se consolida la cultura de preparación ante emergencias tecnológicas, se promueve la actualización constante de la documentación de respaldo y se garantiza que las medidas de recuperación, tanto manuales como automatizadas, sean viables, eficientes y alineadas con los niveles de servicio esperados. En este sentido, las pruebas se convierten en un instrumento de verificación estratégica que aporta confianza, tanto interna como externa, en la capacidad del sistema para enfrentar y superar contingencias de alto impacto.

Nombre de Prueba	Descripción de la prueba	Objetivo de la prueba	Frecuencia
Prueba de escritorio o simulacro teórico (Tabletop test)	Prueba dirigida donde los responsables clave analizan un escenario hipotético de interrupción y revisan sus respuestas de acuerdo con el plan.	Validar comprensión del plan, identificar lagunas y mejorar la coordinación interinstitucional.	Anual

Prueba funcional de procesos manuales	Simulación práctica del uso de procedimientos alternos ante una falla en el sistema (formulario de compra manual, asignación de códigos, rutas físicas de firma)	Asegurar que los procesos de respaldo realmente permiten continuar operaciones críticas.	Cada 6 meses o tras actualizaciones del sistema.
Prueba técnica de restauración (DRP Test)	Activación del plan de recuperación ante desastres (Disaster Recovery Plan), que puede incluir restaurar respaldos, levantar servidores alternos o activar sitios espejo.	Verificar que los datos, sistemas y configuraciones se pueden recuperar en el tiempo previsto.	Anual, idealmente sin previo aviso (prueba sorpresa).
Prueba integral o de interrupción simulada	Simulación integral donde se interrumpe parte del sistema (de forma controlada) para evaluar respuesta de personal, uso de procedimientos manuales y	Medir el desempeño real del plan, incluyendo tiempo de respuesta, comunicación y continuidad.	Cada 2 años (por su complejidad), o tras cambios significativos en infraestructura.

	recuperación final.		

6. Control de versión del documento

Datos relevantes sobre el número de versión del Plan de Continuidad de Negocio				
Versión	**Tarea**	**Responsable**	**Cargo**	**Fecha**
1	Elaboración	Warner Cruz Barboza	Administrador de Catalogo	08/07/2025
	Revisión	Roy Duran Lizano	Asesor de la Unidad de Gestión del SDU	
	Visto bueno	Rosa Chaves Corrales	Directora de Planificación Institucional	
	Aprobación	Yesenia Ledezma Rodriguez	Directora de contratación Pública	
Sitio de almacenamiento (ruta electrónica)				

WARNER CRUZ BARBOZA (FIRMA) PERSONA FISICA, CPF-05-0289-0655. Fecha declarada: 14/07/2025 03:01:02 PM Esta es una representación gráfica únicamente, verifique la validez de la firma.	ROY FRANCISCO DURAN LIZANO (FIRMA) Firmado digitalmente por ROY FRANCISCO DURAN LIZANO (FIRMA) Fecha: 2025.07.14 15:05:41 -06'00'
Elaborado: Wargner Cruz Barboza Unidad de Gestión del SDU	Revisado: Roy Duran Lizano Unidad de Gestión del SDU

YESENIA LEDEZMA RODRIGUEZ (FIRMA) PERSONA FISICA, CPF-01-0852-0779. Fecha declarada: 14/07/2025 06:31:34 PM Esta es una representación gráfica únicamente, verifique la validez de la firma.	ROSA ISELA CHAVES CORRALES (FIRMA) Firmado digitalmente por ROSA ISELA CHAVES CORRALES (FIRMA) Fecha: 2025.07.14 15:15:13 -06'00'
Aprobado: Yesenia Ledezma Rodríguez Directora de Contratación Pública	Visto bueno: Rosa Chaves Corrales Directora de Planificación Institucional