1. OBJETIVO

Establecer las medidas organizacionales, funcionales y tecnológicas para prevenir, detectar, contener y recuperar fallas del Aplicativo, preservando la integridad, trazabilidad, confidencialidad cuando corresponda, disponibilidad y verificabilidad del procedimiento de sorteo; impedir modificaciones de sus condiciones después de conocido el resultado y asegurar la publicación previa del procedimiento aplicable ante fallas tecnológicas.

2. ALCANCE

Aplica desde la preparación y publicación de las reglas del sorteo, verificación de participantes y configuración, hasta la ejecución, consolidación, firma o aprobación del resultado, publicación, custodia de evidencias y retorno a la normalidad. Comprende indisponibilidad de la interfaz, servicio aplicativo, motor de persistencia, conectividad, energía, identidades, integraciones y errores de integridad. Incluye los sorteos que la entidad decida realizar con este aplicativo; no presume la arquitectura física o lógica que no ha sido acreditada.

3. RESPONSABLE

La Dirección de Tecnología de la Información y las Comunicaciones coordina la recuperación técnica conforme al Plan de Recuperación de Desastres (DRP) institucional. El responsable funcional del sorteo dirige la suspensión, continuidad o reprogramación del acto y valida el resultado; la autoridad competente autoriza la reanudación o repetición según las reglas previamente publicadas. Seguridad de la Información asesora en integridad, preservación de evidencia e incidentes. Los nombres y suplencias se obtienen del directorio institucional vigente, sin consignar datos personales en esta guía.

4. DEFINICIONES

Aplicativo Selección de selección auxiliares de la justicia: Solución utilizada para registrar las condiciones y participantes habilitados, ejecutar el mecanismo de selección y generar evidencia del resultado.

- **BIA:** Análisis de impacto al negocio que establece prioridades y tolerancias de interrupción.
- **BCP:** Plan de continuidad de negocio.
- **DRP:** Plan de recuperación ante desastres de tecnología, conforme a GTI-GU-005.
- **RTO:** Tiempo máximo objetivo para restablecer el servicio; debe ser aprobado a partir del BIA.
- **RPO:** Pérdida máxima admisible de información medida en tiempo; no equivale a autorización para perder el resultado de un sorteo.

- **Contingencia:** Interrupción o alteración que impide ejecutar o acreditar el sorteo en las condiciones publicadas.
- **Congelamiento:** Bloqueo de cambios sobre reglas, universo de participantes, criterios y parámetros del sorteo una vez iniciado el acto.
- **Evidencia de sorteo:** Acta, registros de auditoría, sellos de tiempo, valores de integridad, resultado y soportes de aprobación.
- **Punto de control:** Registro verificable de reglas, participantes, configuración, instante de inicio y estado transaccional.

5. CONTENIDO

5.1. GUÍA DEL PLAN DE CONTINGENCIA DEL APLICATIVO DE SELECCIÓN AUXILIARES DE LA JUSTICIA

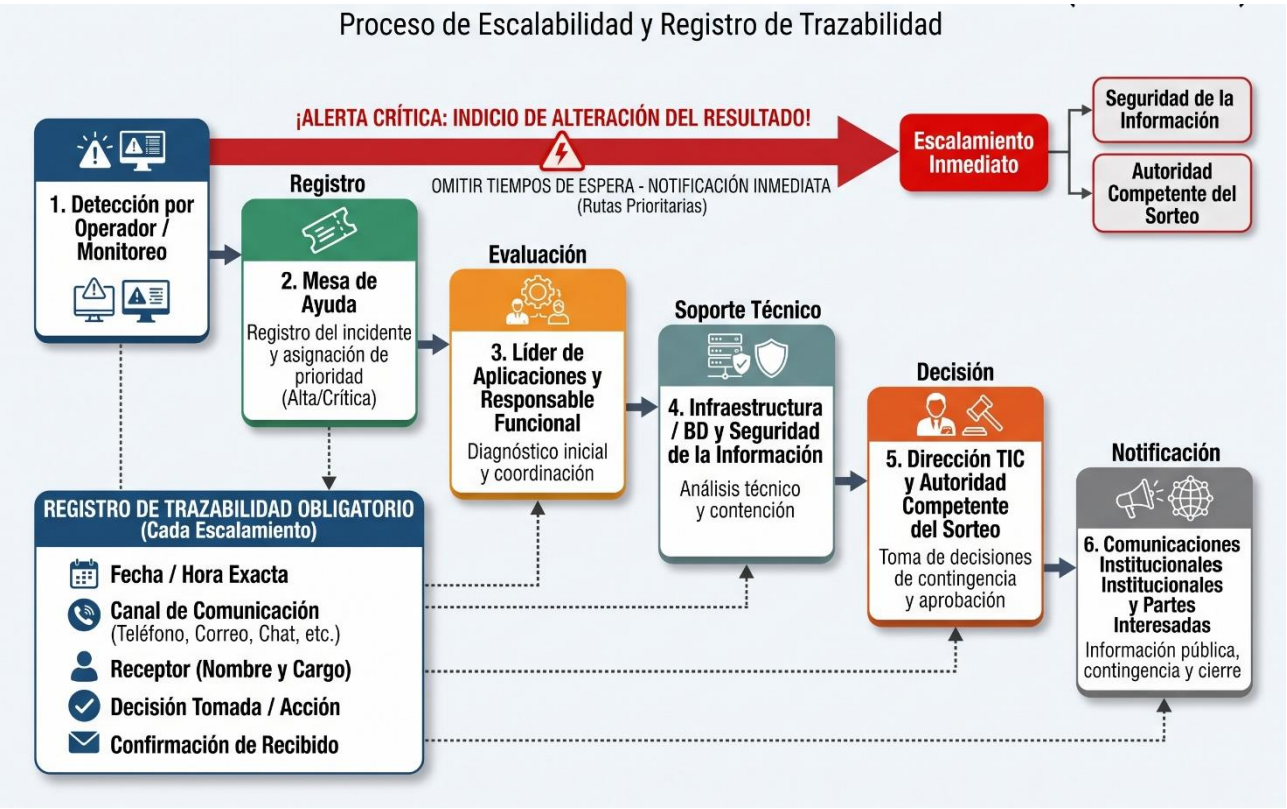
5.1.1. Escenarios de desastre

Escenario	Efecto sobre el sorteo	Medida inicial
Falla de servidor o servicio aplicativo	Interrupción de sesión o ejecución	Suspender operación, registrar estado y evaluar reinicio controlado
Falla de base de datos o almacenamiento	Riesgo de inconsistencia, duplicidad o pérdida de trazas	Bloquear escrituras, preservar logs y verificar consistencia
Pérdida de red o energía	Indisponibilidad parcial o total	Detener el acto y validar conectividad antes de continuar
Ciberataque o acceso no autorizado	Posible alteración de parámetros o resultados	Aislar componentes, activar gestión de incidentes y preservar evidencias
Error de aplicación o ejecución parcial	Resultado incompleto o ambiguo	No ejecutar de nuevo automáticamente; reconstruir el estado transaccional
Falla durante publicación del resultado	Desacuerdo entre resultado confirmado y difundido	Preservar resultado original, verificar firmas y corregir solo el canal de publicación

5.1.2. ROLES Y RESPONSABILIDADES

Rol	Antes	Durante	Después
Responsable funcional	Aprueba reglas y evidencias base; coordina publicación previa	Ordena suspensión, documenta impacto y valida decisión	Acepta integridad del resultado y firma cierre
Líder de aplicaciones	Mantiene configuración y monitoreo	Diagnostica servicio y ejecuta acciones autorizadas	Valida estabilidad y documenta causa raíz
Infraestructura / BD	Verifica copias, capacidad y recuperación	Restaura componentes y comprueba integridad técnica	Reconcilia datos, respaldos y monitoreo
Seguridad de la Información	Define controles de acceso y evidencia	Preserva trazabilidad y atiende sospechas de alteración	Revisa evidencias y lecciones aprendidas
Mesa de ayuda / comunicaciones	Mantiene canales y directorio	Registra incidente y distribuye comunicaciones autorizadas	Actualiza estado y cierre
Autoridad competente del sorteo	Aprueba procedimiento previo	Decide reanudación, suspensión definitiva o repetición conforme a reglas	Aprueba acta final y publicación

5.2. DIAGRAMA DE ESCALAMIENTO ANTE INCIDENTES



5.3. ACTIVIDADES DE NOTIFICACIÓN, EVALUACIÓN Y ACTIVACIÓN DEL PLAN

5.3.1. Notificación

Registrar identificador del incidente, hora de detección, fase del sorteo, servicios afectados, evidencia de pantalla y bitácoras, último estado confirmado y personas presentes. Informar sin difundir datos sensibles ni anticipar resultados no confirmados.

5.3.2. Evaluación y activación

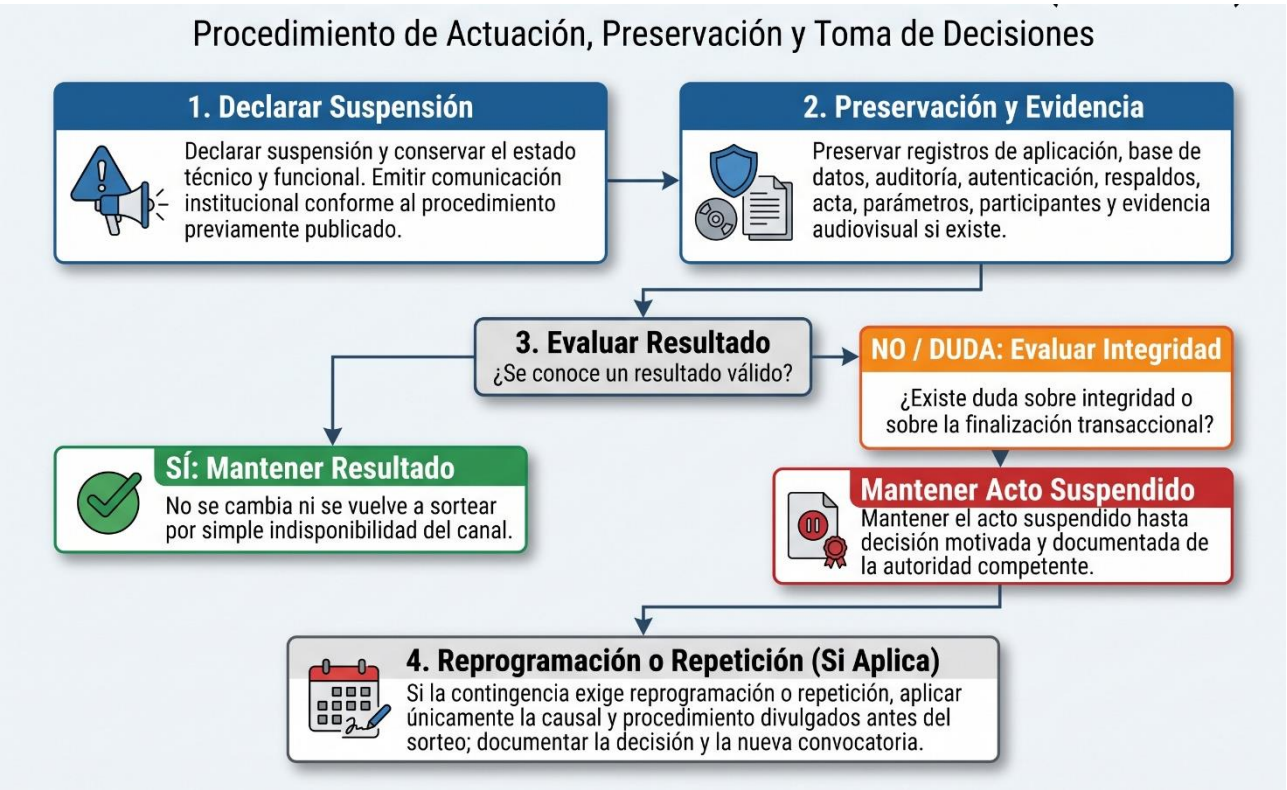
El líder técnico clasifica indisponibilidad, inconsistencia o sospecha de manipulación. El responsable funcional determina si el acto puede suspenderse de forma segura. La autoridad competente activa formalmente la contingencia del sorteo; la DTIC activa el DRP cuando el impacto exceda el aplicativo. Se prohíben reinicios, reprocesos o restauraciones que puedan alterar el resultado sin preservación previa de evidencia y autorización documentada.

5.3.3. Análisis de impacto

Determinar la fase afectada: preparación, cierre del universo, ejecución, confirmación del resultado o publicación. Evaluar efectos sobre integridad, transparencia, igualdad

de condiciones, oportunidad y trazabilidad. El RTO debe establecerse por BIA y ventana del acto; el RPO de los registros críticos debe asegurar que el resultado y las condiciones confirmadas no se pierdan. En ausencia de valores aprobados, prima la suspensión controlada sobre una recuperación apresurada.

5.4. PROTOCOLO DE CONTINGENCIA ANTE INCIDENCIAS



5.5. ACTIVIDADES DE MANTENIMIENTO

Revisar el plan después de cambios de versión, infraestructura, motor de datos, reglas del sorteo, controles de identidad, incidentes o pruebas. Verificar anualmente vigencia de directorios, dependencias, accesos de emergencia, respaldos, registros de auditoría y capacidad de restauración. Los cambios requieren control documental y revisión conjunta funcional–DTIC–Seguridad.

5.6. ACTIVIDADES DE PRUEBA

Ejecutar al menos una prueba anual y antes de sorteos de alta criticidad cuando exista un cambio significativo. La prueba debe usar datos ficticios, no interferir con actos reales y registrar aprobación, escenario, pasos, tiempos, evidencia y hallazgos.

Prueba	Criterio de aceptación
Caída de interfaz antes del inicio	Reanudación sin cambiar reglas ni universo de participantes.
Falla durante la transacción	Ausencia de resultados duplicados y capacidad de establecer estado inequívoco.
Restauración de datos	Conciliación de registros y evidencias con punto de control íntegro.
Pérdida de canal de publicación	Conservación del resultado confirmado y publicación posterior idéntica.
Acceso no autorizado simulado	Alerta, bloqueo, preservación de logs y escalamiento.

5.7. DISTRIBUCIÓN DE LA GUÍA

Distribución controlada al responsable funcional del sorteo, Dirección TIC, líderes de aplicaciones e infraestructura, Seguridad de la Información, mesa de ayuda, autoridad del sorteo y control interno cuando proceda. La versión publicada para participantes contendrá el procedimiento funcional ante fallas, sin detalles de infraestructura, credenciales o configuraciones de seguridad.

5.8. RECURSOS MÍNIMOS REQUERIDOS

- Acceso autorizado al aplicativo, consola de administración y registros de auditoría.
- Inventario técnico vigente de componentes de aplicación, servidores, bases de datos, red y dependencias, administrado conforme a GTI-GU-004.
- Copias de seguridad, herramienta de restauración y evidencia de pruebas según GTI-PR-001.
- Acta y reglas publicadas, padrón/listado de habilitados, parámetros, identificador único de sorteo y evidencia de congelamiento.
- Canal alterno de comunicación institucional y directorio de escalamiento.
- Medio seguro para preservar evidencia y huellas de integridad.

5.9. ACTIVIDADES DE CONTINGENCIA

Etapa / Condición	Acciones Obligatorias y Protocolo de Actuación	Criterio de Control / Decisión
Antes del sorteo	Verificar publicación previa de reglas y procedimiento ante fallas.	Si se presenta indisponibilidad técnica, **suspender el inicio** y anunciar formalmente la

Etapa / Condición	Acciones Obligatorias y Protocolo de Actuación	Criterio de Control / Decisión
	Registrar versión del sistema, hora de cierre, censo de participantes habilitados y parámetros de configuración.	reprogramación conforme a las reglas publicadas.
Durante la ejecución	Interrumpir de inmediato las acciones del operador ante anomalías.	Contención preventiva y aseguramiento de trazabilidad transaccional.
	Registrar hora exacta, estado visible en pantalla y mensajes de error del sistema.	
	Prohibición estricta: No pulsar nuevamente la opción de sortear hasta confirmar el estado de la transacción.	
	Preservar el acta de la sesión y el registro de testigos cuando corresponda.	
Resultado confirmado	Mantener el resultado inmutable.	**Inmutabilidad:** El resultado no se altera ni se repite por simple indisponibilidad del canal de salida/visualización.
	Distinguir técnicamente entre falla de ejecución y falla de visualización / publicación.	
	Rehabilitar exclusivamente el acceso y divulgación del mismo resultado validado.	
Resultado no verificable	Mantener el acto formalmente suspendido.	Toda decisión se rige de manera estricta por las causales y el procedimiento previamente divulgado.
	Apertura inmediata de acta de incidente de seguridad/operación.	
	Escalar a la autoridad competente para determinar la recuperación o repetición.	

5.10 ACTIVIDADES DE CONTINGENCIA TECNOLÓGICAS

Actividad	Acciones Clave y Protocolo Técnico	Referencia / Criterio de Control
Contención	Detener de inmediato operaciones de escritura o transacciones en curso.	Prevención de inconsistencias transaccionales y sorteos duplicados.
	Suspender tareas automáticas de reintento para evitar duplicación de sorteos.	
	Restringir accesos privilegiados según el nivel de riesgo identificado.	
Captura forense y operativa	Exportar registros (*logs*) y evidencias con sellos de tiempo (*timestamps*).	Aseguramiento de trazabilidad y preservación de evidencia técnica/legal.
	Generar hashes de integridad y asegurar cadena de custodia cuando aplique.	
	Preservar el estado exacto de la base de datos previo a cualquier intento de restauración.	
Diagnóstico de capa afectada	Verificar conectividad de red y resolución de nombres (DNS).	Identificación precisa del origen de la falla (infraestructura, red, datos o aplicación).
	Comprobar autenticación y salud general del servicio.	
	Evaluar almacenamiento, transacciones pendientes y enlace con el motor de persistencia (sin asumir tecnología particular).	
Recuperación del servicio	Aplicar procedimientos del fabricante y guías vigentes de despliegue / administración formalmente aprobadas.	Restablecimiento controlado sin afectación colateral de componentes.

Actividad	Acciones Clave y Protocolo Técnico	Referencia / Criterio de Control
	Reiniciar única y exclusivamente los componentes necesarios tras contar con autorización explícita.	
Recuperación de datos	Localizar copia de respaldo válida y verificar consistencia.	**GTI-PR-001** (Procedimiento de Respaldo y Restauración).
	Restaurar en un entorno aislado de pruebas/verificación cuando sea viable.	
	Contrastar registros del sorteo, estado transaccional, resultado final y firmas/huellas antes de promover a producción.	
Validación	Realizar pruebas exhaustivas de lectura, permisos/roles e integridad referencial.	Criterio de aceptación funcional y de seguridad para puesta en producción.
	Confirmar unicidad del resultado, generación de bitácoras y visualización / publicación.	
	Obtener visto bueno y validación conjunta con el responsable funcional antes de reabrir el sistema.	
Escalamiento mayor	Declarar contingencia mayor si la afectación compromete la infraestructura base o servicios compartidos institucionales.	**GTI-GU-005** y procedimientos institucionales de continuidad/DRP aplicables.
	Desplegar protocolos de continuidad y recuperación ante desastres.	

5.11. RETORNO A LA NORMALIDAD

5.11.1. Actividades funcionales

El responsable funcional contrasta las condiciones iniciales publicadas con los parámetros recuperados, el universo de participantes, las evidencias de ejecución y el resultado. Formaliza aceptación del servicio y determina el reinicio del acto, su continuación o la publicación del resultado previamente confirmado, conforme al procedimiento divulgado. Se levanta acta de cierre con causa, cronología, decisiones y evidencia.

5.11.2. Actividades tecnológicas

La DTIC valida salud de componentes, sincronización temporal, integridad y disponibilidad de la base de datos, consistencia de copias, control de acceso, auditoría, conectividad, desempeño y monitoreo. Cierra el incidente, consolida evidencias, define acciones correctivas y actualiza documentación de configuración y recuperación. Ningún dato del resultado puede editarse para forzar una conciliación.

6. REGISTROS

Registro	Finalidad / custodia
Acta de preparación y publicación previa	Evidenciar condiciones y protocolo divulgado; dependencia funcional.
Registro de incidente y escalamiento	Trazabilidad cronológica; mesa de ayuda.
Evidencia técnica y bitácoras	Integridad y diagnóstico; DTIC / Seguridad.
Acta de decisión y resultado	Acreditar suspensión, continuación o repetición; autoridad competente.
Reporte de pruebas y restauración	Verificar efectividad; DTIC.
Informe de cierre y lecciones aprendidas	Mejora continua y acciones correctivas; responsables designados.

7. ANEXOS

- GTI-GU-010 Plan de Contingencia BPM.
- GTI-GU-005 Plan de Recuperación ante Desastres.
- GTI-PR-001 Respaldo y Recuperación de Datos de Infraestructura Tecnológica.
- GTI-GU-004 Gestión de la Configuración.
- GTI-GU-006 Gestión de Incidentes.
- GIN-PO-003 Políticas de Seguridad y Privacidad de la Información del SGSI.

8. CONTROL DE CAMBIOS

Versión	Fecha	Descripción del Cambio
001	09/10/2026	Adaptación de la guía de contingencia al Aplicativo de selección auxiliares de la justicia. Documento de trabajo sujeto a control documental y aprobación institucional.

Elaboró	Revisó	Aprobó
Nombre: Ivan Alexis Ontibon Rojas. **Cargo:** Contratista **Fecha:** 09/10/2026	**Nombre:** Marisol Castiblanco Calixto. **Cargo:** Coordinadora Grupo de Innovación, Desarrollo y Arquitectura de Aplicaciones **Fecha:** 09/10/2026	Nombre: Pacifico Ernesto Barrera Nuban. Cargo: director de Tecnología de la Información y las Comunicaciones (e) Fecha:09/10/2026