PLAN DE RECUPERACIÓN DE DESASTRES (DRP)

DEL PODER JUDICIAL DEL ESTADO DE BAJA CALIFORNIA SUR

La Paz, Baja California Sur, Julio 2023

Tabla de contenido

1.
Introducción

Este documento define el procedimiento para identificar las actividades críticas del Poder Judicial de Baja California Sur y los riesgos a los que se ven expuestas con el fin de determinar planes de acción que permitan una correcta recuperación y continuidad de las mismas ante una interrupción.

2.
Objetivo

El objetivo de un plan de recuperación ante desastres es garantizar que se pueda responder a un desastre u otra emergencia que afecte a los sistemas de información y minimizar el efecto en el funcionamiento de las actividades del Poder Judicial de Baja California Sur. Este documento debe estar resguardado en un lugar seguro y accesible.

Los principales objetivos de este plan de recuperación de desastres, son:

- ➔ Minimizar las interrupciones a las operaciones normales.
- ➔ Limitar el alcance de la interrupción y el daño.
- ➔ Establecer medios alternativos de operación por adelantado.
- ➔ Capacitar al personal con procedimientos de emergencia.
- ➔ Proporcionar una restauración rápida y sin problemas del servicio.

3.
Alcance

Este plan cubre todos los componentes de tecnología que dan soporte a las actividades y servicios ejecutados y provistos por el Poder Judicial de Baja California Sur.

Las actividades y servicios de tecnología provistos por proveedores y provenientes de ambientes externos se encuentran involucrados en este proceso y contempladas sus acciones para garantizar la continuidad.

La actualización de este plan debe realizarse al menos una vez al año.

4.
Definiciones

Plan de Continuidad de Negocios (BCP): Documento donde se detalla el proceso para continuar las operaciones comerciales críticas durante y después de una interrupción del negocio.

Plan de Recuperación de Desastres (DRP): Documento donde se detalla el proceso de recuperación de las herramientas informáticas y tecnológicas de la organización afectadas por un desastre. Es el aspecto tecnológico del BCP.

Objetivo de punto de recuperación (RPO): es la cantidad aceptable de pérdida de datos medida en el tiempo. Por ejemplo, si ocurre un desastre a las 13:00 y el RPO es de una hora, el sistema debe recuperar todos los datos que estaban en el sistema antes de las 12:00. La pérdida de datos abarca solo una hora, entre las 12:00 y las 13:00.

Objetivo de tiempo de recuperación (RTO): se considera el peor escenario, los tiempos máximos se estipulan en caso que resulte necesario algún reproceso, tendrán precedencia los sistemas más críticos.

Es el tiempo que toma después de una interrupción para restaurar un proceso de negocio a su nivel de servicio. Por ejemplo, si ocurre un desastre a las 12:00 y el RTO es de dos horas, el proceso de DR debe restaurar el proceso de negocios al nivel de servicio aceptable para las 14:00.

5.
Estrategia de recuperación

La estrategia de recuperación comienza desde el procedimiento de manejo de incidencias, el cual detecta, escala los requerimientos y define si es necesario iniciar el plan de recuperación y/o el plan de Emergencia y Contingencia.

5.1. Procedimiento de manejo de incidencias

El procedimiento de manejo de incidencias comienza cuando se detecta alguna falla en el sistema que impida el correcto funcionamiento de los usuarios en la plataforma. Si la incidencia afecta la integridad de las personas, entonces se activa el plan de Emergencia y Contingencia. Si la incidencia no se puede resolver en el primer nivel de ayuda, entonces se realiza el escalamiento al encargado de continuidad operacional.

El orden en el cual se realiza el escalamiento de las incidencias se puede ver en la Tabla 1. Este escalamiento se realiza de forma interna. El personal de la Dirección de Informática se debe contactar con el primer nivel de escalamiento de incidencias.

Orden	Encargado	Rol	Puesto	Contacto
1	Jorge Acosta Corona	Líder y Coordinador	Director de Informática del Poder Judicial de B.C.S.	6121315543
2	María José Valencia Araiza	Líder y Gerente de recuperación	Jefe del Departamento de Desarrollo de Sistemas.	6121599199
3	Gabriel Zenen Tiscareño Villorín	Integrante	Jefe del Departamento de Soporte Técnico.	6121524686
3	Javier de Jesús Tadeo Olachea Urías	Integrante	Jefe de Departamento de Redes y Bases de Datos.	6121362448
4	Abraham Guadalupe Carballo González	Integrante	Administrador de Base de Datos.	6121680919

Tabla 1. Orden de escalamiento de incidencias

5.2 Procedimiento de operaciones de respaldo

Para garantizar que se puedan realizar tareas operativas esenciales de procesamiento de datos después de la interrupción. El equipo de la Dirección de Informática del Poder

Judicial de Baja California Sur realiza las siguientes actividades:

- ➔ Todas las noches, toda base de datos es respaldada en un disco duro externo y en un servidor de réplica localizado en el site principal del H. Tribunal Superior de Justica del Estado de B.C.S.
- ➔ Se mantienen los respaldos de los últimos 45 días.

5.3. Procedimientos de acciones de recuperación.

Para facilitar la rápida restauración de un sistema de procesamiento de datos después de un desastre. Todo plan de recuperación ante desastres debe comenzar con la siguiente lista de actividades:

- **A.** Notificar al director de Informática el cual es el encargado de continuidad operacional.
- **B.** Notificar a la presidencia del Tribunal Superior de Justicia de B.C.S.
- **C.** Contactar y configurar el equipo de recuperación de desastres.
- **D.** Determinar el grado de desastre.
- **E.** Implementar un plan de recuperación de aplicaciones adecuado en función del alcance del desastre.
- **F.** Monitorear el progreso.
- **G.** Ponerse en contacto con el sitio de copia de seguridad y establecer horarios. Ponerse en contacto con el resto del personal necesario, tanto el usuario como el equipo técnico.
- **H.** Ponerse en contacto con los proveedores, tanto de hardware como software. Notificar a los usuarios sobre la interrupción del servicio.

5.4. Procedimiento de recuperación ante la indisponibilidad del sistema

En caso de que el servicio no esté recibiendo peticiones se debe:

1. Ingresar a consola del servidor.
2. Revisar alertas y alarmas configuradas en consola.
3. Identificar componentes sin funcionamiento. Si el componente caído es el servicio de base de datos, se debe ir al procedimiento de recuperación ante caída de la base de datos.
    a. Revisar los valores asignados a cada componente.
    b. Realizar imagen de seguridad del componente caído.
    c. Intentar reiniciar el componente caído.
4. Si no hay componentes caídos, pasar a procedimiento de recuperación ante la falla de software.
5. Revisar fallas en grupo de auto escalamiento (que debe levantar instancias de forma automática)
6. En caso de que el componente no pueda ser reiniciado, se debe restaurar desde su última copia de respaldo.
    a. Si la copia de respaldo no soluciona el problema, se debe restaurar desde la última imagen estable de la solución.
7. Realizar pasos 2 a 6 hasta solucionar el problema.
8. Se notifica al responsable operacional y a usuario final.

5.5. Procedimiento de recuperación ante falla en software

Este procedimiento solo se puede ejecutar si el procedimiento de recuperación ante la indisponibilidad del sistema identifica que no existe componente caído. Todo componente debe estar activo.

Pasos a seguir:

1. Contactar al equipo del departamento de desarrollo de sistemas.
2. Realizar respaldo extraordinario de la base de datos.
3. Realizar copia de seguridad del ambiente productivo.
4. Configurar base de datos en ambiente de QA(Aseguramiento de Calidad).
5. Revisar logs del sistema para identificar problemas.
6. Si problema está relacionado a alguna actualización reciente, se debe restaurar software a la versión previa en el ambiente QA
    a. Si se corrige problema en ambiente QA, entonces se debe corregir el software en dicho ambiente, realizando hotfix(parche rápido).
    b. Se ejecutan las pruebas unitarias de la solución.

   c. Si todas las pruebas están correctas y la solución, en ambiente QA, está operativa, entonces se realiza un paso a producción.
   d. Se realizan nuevas pruebas unitarias que eviten que el error se repita en el futuro.
7. Si el problema está relacionado a alguna configuración del sistema,
   a. Replicar las copias de seguridad del ambiente productivo en un ambiente QA.
   b. Realizar pruebas de configuración para identificar problemas.
   c. Corregir problema en ambiente QA.
   d. Realizar pruebas unitarias de la solución.
   e. Realizar pruebas de usuario.
   f. Si no hay errores, se debe realizar paso a producción. En caso contrario, iterar punto 7.
   g. Realizar configuraciones en ambiente productivo.
   h. Documentar error.

8. Se notifica al responsable operacional y a usuario final.

5.6. **Procedimiento de recuperación ante caída de la base de datos**

1. Contactar al equipo del departamento de desarrollo de sistemas y de redes y bases de datos.
2. Realizar respaldo extraordinario de la base de datos.
3. Realizar copia de seguridad de los servidores de base de datos.
4. Restaurar un ambiente de QA de la base de datos. En dicho ambiente revisar que la base de datos tenga espacio disponible en disco.
   a. Corregir espacio si falta.
   b. Revisar logs de la base de datos.
   c. Revisar alertas de ambiente de datos.
   d. Identificar y corregir problemas en base de datos.
   e. Realizar pruebas en ambiente QA. Si fallan las pruebas, volver al punto 4.a.
   f. Realizar paso a producción de modificaciones.
5. Si la base de datos no puede ser corregida, se debe restaurar la última versión respaldada
6. Se notifica al responsable operacional y a usuario final.

6.
RTO y RPO

Se definen los siguientes valores de RTO y RPO para los procesos críticos y que comprometen la operación de la plataforma.

RTO: [6 Horas]

RPO: [2.5 Horas]

7.
Pruebas del plan

El DRP es validado mediante el desarrollo de un ejercicio de prueba de los planes y la tecnología complementaria. Éste se lleva a cabo al menos una vez al año o luego de cambios significativos en la tecnología.

Una vez que se completa el DRP, el coordinador y gerente del equipo de recuperación deben firmar el “Sign Off” (informe de resultado de pruebas) para garantizar que los componentes principales están suficientemente documentados.

8.

Versionado

Confeccionado por:	JAVIER DE JESUS TADEO OLACHEA URIAS
Versión:	1.3
Fecha última de actualización:	12/07/2023
Revisado por:	JORGE ACOSTA CORONA
Aprobado por:	JORGE ACOSTA CORONA