



PROGRAMA DE CONTINUIDAD OPERATIVA Y RECUPERACIÓN ANTE DESASTRES DE LOS SISTEMAS INFORMÁTICOS



**Organismo Operador Municipal del Sistema de
Agua Potable y Alcantarillado de Loreto.**

01 de abril de 20026, Loreto Baja California Sur.



CONTENIDO

- I. FUNDAMENTO JURÍDICO
- II. OBJETIVO
- III. ALCANCE
- IV. IDENTIFICACIÓN DE SISTEMAS CRÍTICOS
- V. ANÁLISIS DE RIESGOS
- VI. MEDIDAS PREVENTIVAS
- VII. ESTRATEGIA DE RESPALDOS
- VIII. CONTINUIDAD DEL SISTEMA DE COBRANZA
- IX. PROCEDIMIENTO DE RECUPERACIÓN
- X. COMITÉ DE CONTINUIDAD OPERATIVA
- XI. PRUEBAS Y SIMULACROS
- XII. REVISIÓN Y ACTUALIZACIÓN



I. FUNDAMENTO JURÍDICO

El presente Programa de Continuidad Operativa y Recuperación ante Desastres de los Sistemas Informáticos del Organismo Operador Municipal del Sistema de Agua Potable y Alcantarillado de Loreto (OOMSAPAL) se emite con fundamento en las siguientes disposiciones jurídicas:

Marco Federal

- Constitución Política de los Estados Unidos Mexicanos, artículo 115, fracción III, inciso a), que establece la prestación del servicio de agua potable como competencia municipal.
- Ley de Aguas Nacionales y su Reglamento – normas aplicables a los organismos operadores de agua.
- Ley General de Contabilidad Gubernamental (LGCG) – establece la obligación de resguardar la información contable y financiera de las entidades públicas.
- Ley Federal de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) – aplicable respecto de la información personal de usuarios y trabajadores administrada por el Organismo.
- NOM-031-CONAGUA-2011 – Sistemas de agua potable, toma domiciliaria y alcantarillado sanitario: hermeticidad.
- Lineamientos emitidos por el Consejo Nacional de Armonización Contable (CONAC) – resguardo de información contable gubernamental.

Marco Estatal – Baja California Sur

- Constitución Política del Estado Libre y Soberano de Baja California Sur, artículos aplicables a la administración pública municipal y prestación de servicios.
- Ley de Aguas de Baja California Sur – establece la organización y atribuciones de los organismos operadores municipales.
- Ley de Transparencia y Acceso a la Información Pública para el Estado de Baja California Sur – obliga a los sujetos obligados a preservar y garantizar la disponibilidad de la información pública.
- Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Baja California Sur (LGPDPPSO-BCS) y normatividad del Instituto de Transparencia y Protección de Datos Personales de Baja California Sur (ITPBCS).
- Ley de Responsabilidades de los Servidores Públicos del Estado de Baja California Sur – responsabilidad en el manejo y resguardo de información institucional.
- Ley de Presupuesto de Egresos, Contabilidad Gubernamental y Gasto Público del Estado de Baja California Sur.

Marco Municipal – Municipio de Loreto

- Bando de Policía y Gobierno del Municipio de Loreto, Baja California Sur – normas de orden público y organización municipal.
- Reglamento Orgánico de la Administración Pública Municipal de Loreto – estructura y atribuciones de las dependencias municipales.



- Estatuto Orgánico del Organismo Operador Municipal del Sistema de Agua Potable y Alcantarillado de Loreto (OOMSAPAL) 2023 – define la estructura orgánica, competencias y responsabilidades del Organismo.
- Reglamento Interior de Trabajo de OOMSAPAL – disposiciones laborales aplicables al personal en situaciones de contingencia.
- Programa Interno de Protección Civil de OOMSAPAL – en coordinación con la Unidad Interna de Protección Civil (UIPC) del Organismo, conforme a la Ley General de Protección Civil y su equivalente estatal.



II. OBJETIVO

Establecer las acciones, procedimientos y responsabilidades necesarias para garantizar la continuidad de los servicios informáticos y la recuperación oportuna de los sistemas críticos del Organismo Operador Municipal del Sistema de Agua Potable y Alcantarillado de Loreto (OOMSAPAL) ante incidentes tecnológicos, desastres naturales, fallas de infraestructura, interrupciones de comunicaciones, siniestros o cualquier evento que afecte la operación institucional, con el fin de asegurar la prestación ininterrumpida del servicio público de agua potable y alcantarillado a la ciudadanía del Municipio de Loreto, Baja California Sur.

III. ALCANCE

El presente Programa aplica a la totalidad de los sistemas, equipos, infraestructura tecnológica y recursos informáticos que soportan los procesos sustantivos y de apoyo de OOMSAPAL, incluyendo:

- Sistema de Cobranza.
- Sistema Contable Gubernamental.
- Sistema de Reportes Institucionales.
- Equipos de cómputo de escritorio y portátiles.
- Servidores locales y equipos de almacenamiento.
- Equipos de comunicaciones (switches, routers, access points).
- Redes institucionales (LAN/WAN).
- Servicios de Internet (Telmex y Starlink).
- Información institucional en todos sus soportes digitales.
- Personal usuario de los sistemas.
- Servicios tecnológicos contratados con terceros.
- Infraestructura tecnológica vinculada a la operación de la Planta de Tratamiento de Aguas Residuales (PTAR).

Este Programa aplica a todas las áreas de OOMSAPAL: Dirección General, Dirección Administrativa, Área Comercial, Dirección Operativa, Departamento de Informática y demás unidades administrativas y operativas del Organismo.



IV. IDENTIFICACIÓN DE SISTEMAS CRÍTICOS

Se identifican como sistemas críticos aquellos cuya interrupción impacta directamente en la prestación del servicio público, la captación de ingresos o el cumplimiento de obligaciones legales del Organismo:

Sistema / Recurso	Criticidad	RTO*	Dependencias principales
Sistema de Cobranza	Muy Alta	4 h	Internet, proveedor externo, infraestructura de comunicaciones
Sistema Contable Gubernamental	Alta	8 h	Equipos locales, respaldos institucionales
Sistema de Reportes Institucionales	Alta	8 h	Infraestructura tecnológica local
Sistemas PTAR (SCADA/control)	Alta	4 h	Red interna, controladores industriales, energía eléctrica
Correo Institucional	Media	24 h	Servidor / Internet
Portal Institucional	Baja	72 h	Servidor / Internet

* RTO: Tiempo Objetivo de Recuperación (Recovery Time Objective).



V. ANÁLISIS DE RIESGOS

Dada la ubicación geográfica del Municipio de Loreto, Baja California Sur, en la costa del Golfo de California, con exposición a fenómenos hidrometeorológicos y sísmicos, se identifican los siguientes riesgos:

5.1 Riesgos Naturales

Sismos

La Península de Baja California se localiza en una zona de alta actividad sísmica, lo que hace de este riesgo una amenaza permanente para la infraestructura de OOMSAPAL.

- Daño a equipos de cómputo y servidores.
- Daño a instalaciones físicas y cableado estructurado.
- Interrupción del suministro eléctrico.
- Pérdida temporal de comunicaciones.
- Suspensión de actividades operativas y administrativas.

Huracanes y Tormentas Tropicales

El Municipio de Loreto se ubica en la franja de trayectoria histórica de ciclones tropicales en el Pacífico mexicano, con temporada activa de junio a noviembre.

- Interrupción prolongada del suministro eléctrico.
- Daños físicos a instalaciones, antenas y cableado exterior.
- Interrupción de los servicios de Internet (Telmex y Starlink).
- Inundaciones en instalaciones del Organismo.
- Imposibilidad de acceso físico a las oficinas durante el evento.
- Afectación a la infraestructura de la PTAR y pozos de abastecimiento.

Calor Extremo y Polvo

Las condiciones climáticas del desierto de Loreto —temperaturas superiores a 45 °C en verano y polvaredas frecuentes— representan un riesgo específico para la vida útil de equipos de cómputo.

- Sobrecalentamiento de servidores y equipos de red.
- Acumulación de polvo en componentes críticos.
- Reducción de vida útil del hardware.

5.2 Riesgos de Infraestructura

Interrupciones Eléctricas

- Apagado inesperado de equipos con pérdida de información en proceso.
- Daño a hardware por variaciones de voltaje.
- Corrupción de bases de datos por apagado abrupto.
- Suspensión temporal de los sistemas de cobranza y contabilidad.

Fallas de Equipos de Red

- Pérdida de conectividad interna y externa.
- Caída de servicios institucionales.
- Interrupción de acceso al Sistema de Cobranza externo.



5.3 Riesgos de Comunicaciones

Escenario	Impacto	Probabilidad	Medida de Mitigación
Falla del servicio Telmex	Pérdida parcial de conectividad	Media	Conmutar a Starlink como servicio de respaldo
Falla del servicio Starlink	Pérdida parcial de conectividad	Baja	Operar mediante Telmex como servicio principal
Falla simultánea de ambos servicios	Imposibilidad total de acceso a sistemas externos	Muy Baja	Activar modo de operación offline y registros manuales

5.4 Riesgos de Terceros

Indisponibilidad del Sistema de Cobranza

El sistema de cobranza de OOMSAPAL se encuentra alojado y administrado por un proveedor externo, lo que implica dependencia de la disponibilidad de su infraestructura.

- Falla del servidor o centro de datos del proveedor.
- Mantenimiento no programado por parte del proveedor.
- Ataques informáticos al servidor del proveedor.
- Problemas de conectividad en el extremo del proveedor.
- Errores de configuración o actualizaciones fallidas.

Consecuencias para OOMSAPAL:

- Suspensión temporal de la cobranza a usuarios del Municipio de Loreto.
- Retraso en la atención al público.
- Afectación en la captación de ingresos propios del Organismo.
- Incumplimiento temporal de las metas de cobranza establecidas por la Junta de Gobierno.

5.5 Riesgos de Seguridad Física

Robo de Equipos

- Pérdida de información institucional y de usuarios.
- Necesidad de sustitución de equipos y restauración de respaldos.
- Interrupción de operaciones administrativas.

Medidas preventivas implementadas:

- Sistema de videovigilancia en instalaciones del Organismo.
- Guardia de seguridad en horario nocturno.
- Control de acceso a oficinas y áreas de servidores.

Incendios

- Daño o destrucción de equipos de cómputo.
- Pérdida irreversible de información.
- Suspensión prolongada de operaciones.



Medidas preventivas implementadas:

- Extintores ubicados estratégicamente en las instalaciones.
- Revisión periódica de instalaciones eléctricas.
- Capacitación al personal para uso de extintores.
- Coordinación con la Unidad Interna de Protección Civil (UIPC) de OOMSAPAL.

5.6 Riesgos Informáticos

- Malware y virus informáticos.
- Ransomware (secuestro de información).
- Phishing y suplantación de identidad digital.
- Accesos no autorizados a sistemas institucionales.
- Eliminación accidental o intencional de información.
- Vulnerabilidades en sistemas desactualizados.



VI. MEDIDAS PREVENTIVAS

6.1 Seguridad Física

- Operación continua del sistema de videovigilancia en instalaciones de OOMSAPAL.
- Guardia de seguridad en horario nocturno.
- Control de acceso a áreas administrativas y cuartos de servidores.
- Resguardo de equipos críticos bajo llave en espacios designados.
- Señalización de rutas de evacuación conforme al Programa Interno de Protección Civil.
- Revisión periódica de instalaciones eléctricas por personal calificado.

6.2 Seguridad Informática

- Antivirus institucional actualizado en todos los equipos.
- Firewall configurado en la infraestructura de red.
- Actualizaciones periódicas de sistemas operativos y aplicaciones.
- Control de usuarios y contraseñas con política de caducidad.
- Monitoreo de accesos a sistemas críticos.
- Restricción de instalación de software no autorizado.
- Capacitación al personal en prevención de phishing y seguridad digital.

6.3 Continuidad de Comunicaciones

- Servicio principal de Internet mediante Telmex.
- Servicio secundario de Internet mediante Starlink.
- Configuración de redundancia y failover automático entre ambos servicios.
- Revisión mensual del estado de los equipos de comunicaciones.

6.4 Protección Eléctrica

- Uso de UPS (Sistema de Alimentación Ininterrumpida) para equipos críticos: servidores, switches y equipos de seguridad.
- Supresores de picos de voltaje en equipos de cómputo.
- Procedimiento de apagado controlado ante contingencias eléctricas prolongadas.
- Revisión semestral del estado de las baterías de los UPS.

6.5 Protección ante Condiciones Climáticas de Loreto

- Mantenimiento preventivo de sistemas de climatización en cuartos de servidores.
- Limpieza periódica de filtros y componentes de equipos de cómputo.
- Protocolo de protección de equipos ante alertas por fenómenos hidrometeorológicos emitidas por la Protección Civil Municipal de Loreto.
- Coordinación con la UIPC de OOMSAPAL para activación de protocolos ante huracanes y eventos climáticos extremos.



VII. ESTRATEGIA DE RESPALDOS

7.1 Regla 3-2-1

OOMSAPAL implementará la regla estándar 3-2-1 para la gestión de respaldos de información:

- Tres copias de la información.
- Dos medios distintos de almacenamiento.
- Una copia externa (fuera de las instalaciones del Organismo).

7.2 Información Sujeta a Respaldo

- Sistema Contable Gubernamental.
- Sistema de Reportes Institucionales.
- Documentación institucional digital (contratos, acuerdos, expedientes).
- Configuraciones de red y equipos críticos.
- Base de datos de usuarios del servicio de agua potable y alcantarillado.
- Información de nómina y recursos humanos.
- Información financiera y presupuestal sujeta a la LGCG y normatividad CONAC.

7.3 Frecuencia de Respaldo

Tipo de Respaldo	Frecuencia	Medio	Responsable
Respaldo operativo (sistemas activos)	Diario automático	Disco externo / NAS local	Depto. Informática
Respaldo semanal incremental	Semanal	Unidad extraíble resguardada	Depto. Informática
Respaldo mensual de archivo histórico	Mensual	Almacenamiento externo / nube	Depto. Informática
Respaldo de documentos institucionales	Quincenal	Unidad extraíble fuera de instalaciones	Área Administrativa

7.4 Verificación de Respaldos

- El Departamento de Informática verificará la integridad de los respaldos al menos una vez al mes mediante prueba de restauración parcial.
- Se registrará cada verificación en la Bitácora de Respaldos del Organismo.
- Los respaldos externos fuera de las instalaciones serán resguardados en un lugar seguro designado por la Dirección General.



VIII. CONTINUIDAD DEL SISTEMA DE COBRANZA

Dado que el Sistema de Cobranza de OOMSAPAL se encuentra alojado y administrado por un proveedor externo, su disponibilidad depende tanto de la conectividad a Internet del Organismo como de la infraestructura del proveedor. Se establecen las siguientes disposiciones:

8.1 Responsabilidades del Departamento de Informática

- Mantener actualizados los datos de contacto del proveedor del sistema (teléfono, correo electrónico, mesa de ayuda).
- Conservar copia de los contratos y acuerdos de nivel de servicio (SLA) vigentes.
- Solicitar anualmente al proveedor evidencia de respaldos y planes de disponibilidad.
- Registrar todos los incidentes relacionados con el servicio en la Bitácora de Incidencias Tecnológicas.
- Verificar mensualmente la vigencia de licencias y accesos al sistema.

8.2 Procedimiento ante Falla del Sistema de Cobranza

Paso	Acción	Responsable
1	Verificar conectividad local (LAN/Internet).	Depto. Informática
2	Verificar funcionamiento del servicio Telmex.	Depto. Informática
3	Verificar funcionamiento del servicio Starlink.	Depto. Informática
4	Confirmar si la falla corresponde al proveedor externo.	Depto. Informática
5	Generar reporte de incidencia con hora, descripción y evidencia.	Depto. Informática
6	Contactar al proveedor y solicitar atención inmediata conforme al SLA.	Depto. Informática
7	Activar registro manual de pagos en ventanilla (formato impreso autorizado).	Área Comercial
8	Informar a la Dirección General y al Área Comercial sobre la contingencia.	Depto. Informática
9	Monitorear restablecimiento del servicio y capturar registros manuales al sistema.	Área Comercial / Informática



IX. PROCEDIMIENTO DE RECUPERACIÓN

Se establecen tres niveles de incidente con procedimientos específicos de respuesta y recuperación:

Nivel 1 – Incidente Menor

Ejemplos	Falla de equipo individual, error de usuario, corte breve de luz.
RTO	Hasta 4 horas.
Acciones	Diagnóstico, reinicio o sustitución de equipo, restauración desde respaldo local, registro en bitácora.
Responsable	Departamento de Informática.

Nivel 2 – Incidente Moderado

Ejemplos	Daño de equipo de red, falla de servidor local, pérdida parcial de información, caída del sistema de cobranza por más de 4 horas.
RTO	Hasta 24 horas.
Acciones	Activar registros manuales, contactar proveedores, restaurar desde respaldo, notificar a Dirección General, documentar incidente.
Responsable	Departamento de Informática con apoyo de áreas afectadas.

Nivel 3 – Desastre Mayor

Ejemplos	Huracán, sismo severo, incendio en instalaciones, robo de equipos críticos, caída prolongada del proveedor de cobranza.
RTO	Hasta 72 horas.
Acciones	Activar el Comité de Continuidad Operativa. Evaluar daños. Operar en modo manual. Adquirir equipo de reemplazo. Restaurar desde respaldo externo. Coordinar con Protección Civil Municipal de Loreto y UIPC de OOMSAPAL. Levantar acta de hechos.
Responsable	Director General, con apoyo de todos los departamentos.



X. COMITÉ DE CONTINUIDAD OPERATIVA

Se integra el Comité de Continuidad Operativa de OOMSAPAL, responsable de coordinar la respuesta y recuperación ante contingencias tecnológicas:

Rol / Cargo	Función en el Comité	Responsabilidades principales
Director General	Presidente del Comité	Autorizar la activación del Programa. Emitir declaratoria de contingencia. Comunicar a la Junta de Gobierno.
Director Administrativo	Secretario Técnico	Coordinar recursos administrativos y financieros para la recuperación. Gestionar adquisiciones de emergencia.
Departamento de Informática	Coordinador Técnico	Dirigir la recuperación tecnológica. Ejecutar el presente Programa. Comunicar estado de avance al Comité.
Área Comercial	Enlace Operativo	Garantizar la continuidad de la cobranza. Activar registros manuales. Informar a usuarios del servicio.
Área Administrativa / Contable	Enlace Administrativo	Garantizar la continuidad de los procesos contables. Resguardar documentación física.
Dirección Operativa / PTAR	Enlace Operativo	Coordinar la continuidad de los procesos operativos de distribución de agua y tratamiento de aguas residuales.
UIPC – Unidad Interna de Protección Civil	Coordinación de Seguridad	Articular acciones con la Protección Civil Municipal de Loreto. Activar brigadas de emergencia del Organismo.



XI. PRUEBAS Y SIMULACROS

Con el fin de validar la efectividad del presente Programa y asegurar que el personal conozca los procedimientos de recuperación, se realizarán las siguientes actividades de forma periódica:

Actividad	Periodicidad	Responsable	Registro
Prueba de respaldo y restauración de sistemas	Semestral	Depto. Informática	Acta de prueba
Prueba de conmutación Telmex-Starlink	Semestral	Depto. Informática	Acta de prueba
Simulacro de pérdida de energía eléctrica	Anual	Depto. Informática	Bitácora
Simulacro de sismo (coordinado con Protección Civil Municipal de Loreto)	Conforme a programas institucionales	UIPC / Dirección General	Acta de simulacro
Verificación de integridad de respaldos	Mensual	Depto. Informática	Bitácora de respaldos

Los resultados de cada prueba y simulacro serán documentados y resguardados por el Departamento de Informática. Las observaciones derivadas servirán de base para la mejora continua del presente Programa.



XII. REVISIÓN Y ACTUALIZACIÓN

El presente Programa deberá revisarse y actualizarse al menos una vez al año o cuando se presente alguna de las siguientes condiciones:

- Se implementen nuevos sistemas o aplicaciones informáticas en el Organismo.
- Existan cambios en la infraestructura tecnológica de OOMSAPAL.
- Ocurran incidentes tecnológicos relevantes que evidencien la necesidad de ajustes.
- Cambien las condiciones operativas o normativas aplicables (federales, estatales o municipales).
- Se produzcan cambios en los proveedores de servicios tecnológicos contratados.
- Se modifique la estructura orgánica de OOMSAPAL conforme a su Estatuto Orgánico.
- La Junta de Gobierno emita acuerdos que impliquen modificaciones en materia tecnológica.

Las revisiones y actualizaciones deberán ser formalizadas mediante firma del Director General y quedar registradas en el control de versiones del presente documento.

01 de abril de 2026, Loreto Baja California Sur.

Elaboró	Revisó	Autorizó
Ing. Jesus Rodriguez Manriquez Jefe de Informatica/ Lic. Vicente Benítez de la Cruz Titular del Organo Interno de Control del OOMSAPAL	L.C. Luis Felipe Amador Estrada Director Administrativo del OOMSAPAL	Ing. Luis Miguel Acosta Acosta Director General del OOMSAPAL
 		 