



LINEAMIENTOS DE SEGURIDAD PARA LOS SISTEMAS INFORMÁTICOS Y DE COMUNICACIONES DEL OOMSAPAL



**ORGANISMO OPERADOR MUNICIPAL DEL SISTEMA DE AGUA POTABLE Y
ALCANTARILLADO DE LORETO.**

01 de abril de 2026, Loreto, Baja California Sur.



CONTENIDO

PRESENTACIÓN

MISIÓN

VISIÓN

OBJETIVO

- CAPÍTULO I — DISPOSICIONES GENERALES
- CAPÍTULO II — DEL BUEN USO DE LOS ACTIVOS INFORMÁTICOS
- CAPÍTULO III — CLASIFICACIÓN DE LA INFORMACIÓN
- CAPÍTULO IV — INTERCAMBIO DE INFORMACIÓN Y PRESTACIÓN DE SERVICIOS
- CAPÍTULO V — PROTECCIÓN CONTRA CÓDIGO MALICIOSO (VIRUS Y MALWARE)
- CAPÍTULO VI — SERVICIOS INFORMÁTICOS EN LA RED
- CAPÍTULO VII — USO DE CUENTAS DE USUARIO
- CAPÍTULO VII I— MONITOREO DEL USO DE LOS SERVICIOS INFORMÁTICOS
- CAPÍTULO IX — DEL SISTEMA DE VIDEOVIGILANCIA
- CAPÍTULO X — MARCO JURÍDICO APLICABLE
- CAPÍTULO XI — DISPOSICIONES FINALES



PRESENTACIÓN

El Organismo Operador Municipal del Sistema de Agua Potable, Alcantarillado y Saneamiento de Loreto, Baja California Sur (OOMSAPAL), consciente de la importancia que tienen las tecnologías de la información y comunicación en el desempeño de sus funciones administrativas y operativas, presenta los siguientes Lineamientos de Seguridad para los Sistemas Informáticos y de Comunicaciones.

El presente documento tiene como finalidad establecer las normas, criterios y responsabilidades que deberá observar el personal directivo, administrativo y operativo del Organismo, así como las terceras personas, proveedores y contratistas relacionados con éste, para el uso adecuado y seguro de los recursos tecnológicos, la información institucional y los servicios digitales con que cuenta el OOMSAPAL, contribuyendo así a la protección de su infraestructura informática y al fortalecimiento de una cultura de seguridad de la información.

MISIÓN

Brindar a la ciudadanía del municipio de Loreto, Baja California Sur, servicios de agua potable, alcantarillado y saneamiento con calidad, eficiencia y sustentabilidad, mediante el uso responsable de la infraestructura, los recursos humanos, financieros y tecnológicos del Organismo, contribuyendo al bienestar y desarrollo de la comunidad.

VISIÓN

Ser un Organismo Operador reconocido por la calidad y continuidad de sus servicios de agua potable, alcantarillado y saneamiento, así como por la modernización y seguridad de su infraestructura tecnológica, que garantice la protección de la información institucional y de los datos personales de los usuarios, fortaleciendo la confianza ciudadana y la transparencia en su gestión.

OBJETIVO

Estos Lineamientos tienen como objetivo establecer las disposiciones generales y específicas que regulan el uso, administración, protección y resguardo de los activos informáticos, sistemas, redes, información y servicios tecnológicos del OOMSAPAL, a fin de salvaguardar su confidencialidad, integridad y disponibilidad, prevenir riesgos de seguridad informática, y promover una cultura de uso responsable de la tecnología entre el personal directivo, administrativo y operativo del Organismo, así como entre terceros, proveedores y contratistas que tengan relación con sus servicios e infraestructura.



CAPÍTULO I

DISPOSICIONES GENERALES

Artículo 1.. Los presentes Lineamientos de Seguridad para los Sistemas Informáticos y de Comunicaciones tienen como objetivo promover el buen uso y cuidado de los recursos tecnológicos entre el personal directivo, administrativo y operativo del Organismo Operador Municipal del Sistema de Agua Potable y Alcantarillado de Loreto, Baja California Sur (OOMSAPAL). Las disposiciones de los presentes Lineamientos son de observancia general y tienen por objeto proteger los componentes de los recursos y sistemas informáticos, así como la confidencialidad, integridad y disponibilidad de la información del Organismo.

Los presentes Lineamientos norman la manera en que el OOMSAPAL previene, protege y administra los riesgos relacionados con las tecnologías de información en sus instalaciones, equipos, información, servicios y soluciones informáticas, incluyendo aquellos sistemas de telemetría, control y monitoreo asociados a la operación de los servicios de agua potable, alcantarillado y saneamiento.

Artículo 2.. Todo el personal del OOMSAPAL, así como las terceras personas, proveedores y contratistas relacionados con el Organismo que hagan uso de sus servicios e infraestructura de cómputo y comunicaciones, deben dar cumplimiento a los presentes Lineamientos; tanto en el interior de las instalaciones como en el exterior; de manera física y lógica vía internet.

Artículo 3.. El presente documento deberá ser revisado y actualizado cuando se considere necesario por el departamento de Informática del OOMSAPAL, o por el área que realice dichas funciones, debiendo mantenerse en concordancia con la normatividad estatal y municipal vigente en materia de transparencia, protección de datos personales y administración pública.

Artículo 4.. Para los efectos de los presentes Lineamientos, se entenderá por:

Antivirus. - Software especializado diseñado para detectar, eliminar y prevenir virus informáticos en los dispositivos de la Red.

Activo informático. - Recursos de sistemas informáticos o relacionados con éste, necesarios para el desempeño de las funciones del usuario, tales como equipos de cómputo, impresoras, video proyectores, pantallas, teléfonos, equipos de telecomunicaciones, software, información, así como equipos de telemetría y control operativo, entre otros.

Ayuntamiento. - El H. Ayuntamiento del Municipio de Loreto, Baja California Sur.

Contraseña. - Palabra clave mediante la cual el usuario puede tener acceso a una aplicación, archivo informático o sistema de información.

Correo Electrónico. - Servicio de la Red que permite a los usuarios enviar y recibir mensajes y archivos rápidamente mediante sistemas de comunicación electrónicos.

DI. - Departamento de Informática del OOMSAPAL, o aquella unidad administrativa que realice dichas funciones.

Equipo de Cómputo. - Dispositivo electrónico de uso personal o institucional capaz de almacenar información, procesar datos y entregar al usuario los resultados de la información procesada.

Equipo móvil. - Todo activo informático físico que tiene la facilidad de movilidad, como laptops, tabletas, teléfonos inteligentes, entre otros.



Firewall. - Software o dispositivo especializado de protección, también llamado cortafuegos, cuya función es prevenir y proteger un equipo de cómputo o una red privada de intrusiones o ataques a través de una conexión de red, bloqueando el acceso no autorizado.

Hardware. - Conjunto de elementos físicos o materiales que constituyen una computadora o un sistema informático.

Infraestructura. - Conjunto de bienes informáticos, cableado, equipos de cómputo, dispositivos de red, servidores, sistemas de telemetría y otros equipos de naturaleza tecnológica del OOMSAPAL.

Información reservada y/o confidencial. - Aquella información clasificada como reservada o confidencial conforme a la Ley de Transparencia y Acceso a la Información Pública del Estado de Baja California Sur y a la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Baja California Sur, cuya divulgación pudiera causar un daño al interés público, a la seguridad del Organismo o a los derechos de los titulares de datos personales.

Internet. - Red informática mundial, descentralizada, formada por la conexión directa entre computadoras mediante un protocolo especial de comunicación.

Malware. - Cualquier tipo de software malicioso diseñado para infiltrarse en un dispositivo sin conocimiento ni consentimiento del usuario.

OOMSAPAL. - Organismo Operador Municipal del Sistema de Agua Potable y Alcantarillado de Loreto, Baja California Sur.

Privilegio. - Derecho de un usuario a realizar una tarea específica, que suele afectar a un sistema completo en lugar de un objeto determinado. Los privilegios los asignan los administradores a usuarios individuales o grupos de usuarios, como parte de la configuración de seguridad del equipo.

Servidor. - Equipo de cómputo de altas prestaciones que forma parte de una red y provee servicios a otros equipos denominados clientes.

Servicio informático. - Bien intangible que se proporciona para satisfacer los requerimientos de los usuarios, relacionado con el uso de un activo informático.

Sistema Operativo. - Programa o conjunto de programas informáticos que gestiona los recursos de Hardware y provee servicios a los programas de aplicación, ejecutándose en modo privilegiado respecto de los restantes.

Software. - Conjunto de programas y rutinas que permiten a la computadora realizar determinadas tareas.

Software institucional. - Aplicación o programa informático con licenciamiento de uso propietario que puede ser instalado y utilizado por los usuarios para el desempeño de sus actividades o funciones, o para la gestión de un servicio informático otorgado por el OOMSAPAL.

Software libre. - También conocido como freeware, shareware o software demo. Software gratuito proveniente de internet o cualquier otro medio que no requiere la compra de una licencia para su uso.

Usuario. - Toda persona que haga uso de los activos o servicios informáticos del OOMSAPAL, para el desempeño de sus funciones, consulta o servicio.



Virus. - Software creado para producir daño en un equipo informático.

Web, www (World Wide Web). - Convergencia de conceptos computacionales para presentar y enlazar información que se encuentra dispersa a través de Internet en una forma fácilmente accesible.

CAPÍTULO II DEL BUEN USO DE LOS ACTIVOS INFORMÁTICOS

Artículo 5.. Los usuarios que tengan un activo informático asignado de manera personal para el uso de sus funciones son los únicos responsables de su utilización, así como de la información contenida en éste, por lo que deben evitar compartirlo. En caso de requerir compartirlo o prestarlo, será solamente para cuestiones laborales y sin liberarlo de su responsabilidad.

Únicamente al personal adscrito al OOMSAPAL se podrá asignar responsiva de activos informáticos, misma que deberá quedar por escrito.

Artículo 6.. Toda movilización de activo informático dentro o fuera de las instalaciones del Organismo es responsabilidad del usuario responsable de su resguardo.

Para el caso de equipos de telecomunicaciones, entre ellos switches, puntos de acceso, ruteadores y equipos de telemetría asociados a la operación de los sistemas de agua potable, alcantarillado y saneamiento, su movilización deberá ser bajo supervisión de la DI.

CAPÍTULO III CLASIFICACIÓN DE LA INFORMACIÓN

Artículo 7.. El responsable de un servicio informático ofrecido por el OOMSAPAL es responsable de la información que dicho servicio genera y procesa.

Artículo 8.. Los titulares de cada área, coordinación o departamento deben informar a sus colaboradores sobre la clasificación de la información a su cargo para su adecuado tratamiento, conforme a la Ley de Transparencia y Acceso a la Información Pública del Estado de Baja California Sur.

Artículo 9.. Todo usuario es responsable del resguardo de los datos y debe vigilar que la información esté protegida para asegurar su integridad, disponibilidad y confidencialidad, acorde a su clasificación.

La información puede estar disponible de manera electrónica, impresa en papel, magnética, o bien, en algún otro medio.

Artículo 10.. Todo usuario deberá hacer uso de la información a la que tenga acceso, únicamente para propósitos relacionados con el cumplimiento de sus funciones, debiendo resguardar principalmente la relativa a datos personales de los usuarios del servicio de agua potable, alcantarillado y saneamiento, así como del personal del Organismo, absteniéndose de comunicarla a terceros sin el consentimiento expreso de la persona titular o sin que medie



disposición legal expresa, en términos de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Baja California Sur.

Artículo 11.. Todos los usuarios que hagan uso de información clasificada como reservada, restringida o confidencial deberán evitar que sea accedida por personas no autorizadas y deberán asegurar que se solicite un medio de autenticación para su acceso.

CAPÍTULO IV INTERCAMBIO DE INFORMACIÓN Y PRESTACIÓN DE SERVICIOS

Artículo 12.. Los usuarios que intercambien información que haya sido declarada reservada y/o confidencial, con personal del OOMSAPAL, del H. Ayuntamiento de Loreto o con terceras personas, deberán asegurarse de dejar el registro correspondiente de la entrega de la información proporcionada, ya sea por medio físico o electrónico.

Artículo 13.. Todo convenio del OOMSAPAL con empresas, dependencias, otros organismos operadores o terceras personas para compartir información reservada y/o confidencial deberá apegarse a las disposiciones de la Ley General de Transparencia y Acceso a la Información Pública, la Ley de Transparencia y Acceso a la Información Pública del Estado de Baja California Sur, la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Baja California Sur, debiéndose asegurar que en el convenio se incluyan cláusulas de confidencialidad de la información.

Artículo 14.. Todo proveedor que entregue o proporcione servicios y/o equipamiento informático al OOMSAPAL y que tenga acceso a información reservada y/o confidencial deberá apegarse a las disposiciones legales aplicables en materia de acceso a la información pública y protección de datos personales, y contar con acuerdos de confidencialidad y no divulgación que protejan los intereses del Organismo.

Artículo 15.. Todo servicio y/o equipo informático otorgado por terceros debe ser monitoreado y revisado por la persona responsable de su contratación, para asegurar el cumplimiento de los términos estipulados en los acuerdos, convenios o contratos celebrados por el OOMSAPAL.

CAPÍTULO V PROTECCIÓN CONTRA CÓDIGO MALICIOSO (VIRUS Y MALWARE)

Artículo 16.. Todo equipo de cómputo institucional debe contar con software antivirus y antimalware definido por el Departamento de Informática, así como estar protegido por el firewall del sistema operativo. Si el software antivirus no cubre la plataforma utilizada, el personal deberá notificar a el Departamento de Informática para buscar una alternativa de solución.

Los accesos a internet en cada unidad administrativa del OOMSAPAL deberán tener activo un firewall, el cual debe ser administrado por el Departamento de Informática.

Artículo 17.. Todo usuario que identifique una anomalía en su equipo de cómputo deberá reportarla de inmediato a el Departamento de Informática, para su atención oportuna.



CAPÍTULO VI

SERVICIOS INFORMÁTICOS EN LA RED

Artículo 18.. Todo el personal y terceros son responsables del buen uso de los servicios informáticos alojados en las instalaciones de el Departamento de Informatica y en la nube, asignados para realizar sus funciones administrativas y operativas.

Artículo 19.. Sólo el personal de el Departamento de Informatica queda facultado para acceder a los equipos de cómputo institucionales, para:

- Ejecutar las tareas del procedimiento de mantenimiento preventivo y correctivo.
- Realizar modificaciones al Sistema Operativo.
- Realizar una revisión de seguridad informática y descartar uso indebido (daños intencionales a información o hardware) del equipo de cómputo.

Artículo 20.. Todo titular de área o departamento es responsable de autorizar el acceso al equipo de cómputo que tiene asignado, para que el personal a su cargo realice sus funciones.

Artículo 21.. Ninguna persona debe ver, copiar, alterar o destruir la información que reside en los equipos de cómputo y servidores sin el consentimiento explícito del responsable del equipo o del dueño de la información, excepto en los casos especificados en el artículo 19 del presente documento.

Artículo 22.. Los sistemas institucionales deberán ser accedidos con cuentas que permitan identificar al usuario y deberán estar protegidas con contraseñas seguras. El desarrollo, implementación y vigilancia del acceso seguro en los sistemas institucionales será responsabilidad de el Departamento de Informatica.

Todas las cuentas de usuario y su respectiva contraseña de acceso a los sistemas y servicios de información del OOMSAPAL son personales, permitiéndose su uso bajo la responsabilidad del usuario, única y exclusivamente durante la vigencia de sus derechos. La vigencia de las cuentas de usuario es facultad de el Departamento de Informatica, las cuales son habilitadas, suspendidas o canceladas en consideración a las solicitudes, necesidades y conductas de los usuarios.

Artículo 23.. Toda utilización de herramientas tales como analizadores, escaneo y monitoreo de red, está permitida únicamente para las funciones de administración de las tecnologías de información por parte de el Departamento de Informatica.

Artículo 24.. El equipo de cómputo institucional (computadoras de escritorio y portátiles) será configurado solamente por personal de el Departamento de Informatica para brindar acceso a la red institucional. Todo usuario se abstendrá de realizar cambios en configuraciones de esta naturaleza; en caso de falla o error de acceso a internet por esta causa, será el único responsable.

Artículo 25.. A toda persona que deje de laborar o tener relación con el OOMSAPAL, le será cancelado de manera definitiva su acceso a los recursos informáticos institucionales. El área de Administración y Recursos Humanos comunicará a el Departamento de Informatica toda alta, baja o cambio de personal, para que se tomen las medidas correspondientes de acceso a los servicios de red y comunicación.



Artículo 26.. Todo hardware y software de uso administrativo que sea considerado de riesgo para la seguridad de los servicios informáticos institucionales deberá ser utilizado en ambiente aislado.

Se consideran Hardware de riesgo, de manera enunciativa más no limitativa, los ruteadores, switches, servidores, firewalls, balanceadores de carga, módems y equipos de telemetría y control de procesos operativos.

Se consideran software de riesgo, de manera enunciativa más no limitativa, los analizadores de tráfico de red, herramientas de análisis y diagnóstico de equipos de cómputo, y los demás que determine la persona encargada de el Departamento de Informatica.

CAPÍTULO VII USO DE CUENTAS DE USUARIO

Artículo 27.. El acceso a los sistemas institucionales de información y correo electrónico será a través de una cuenta institucional, compuesta por nombre de usuario y contraseña.

Artículo 28.. Toda solicitud de alta, baja o cambio de privilegios de cuentas del personal administrativo, para acceder a los servicios informáticos, debe ser realizada por el jefe inmediato o jefe de área, debidamente justificada.

Artículo 29.. Todo usuario debe actualizar la contraseña de su cuenta de acceso a los servicios informáticos por lo menos una vez al año, o cuando sospeche que pueda estar comprometida.

Artículo 30.. Cuando se requiera acceder a información de un equipo de cómputo de una persona ausente, ya sea por cuestiones de salud, por estar comisionado en actividades fuera de su área de trabajo u otro motivo no especificado, el responsable del área correspondiente deberá solicitar al encargado de el Departamento de Informatica que se brinde el acceso correspondiente, para dar continuidad a algún proceso institucional. El personal de el Departamento de Informatica únicamente proporcionará acceso al responsable del área que lo haya solicitado, a efecto de que sustraiga la información necesaria, dejando constancia de ello por escrito y con firma del solicitante.

Si una persona deja de laborar, se ausenta del Organismo o cambia de puesto, el jefe inmediato podrá solicitar a el Departamento de Informatica el acceso al equipo institucional que ésta tenía asignado, el cual será concedido para que sustraiga la información pertinente.

CAPÍTULO VIII MONITOREO DEL USO DE LOS SERVICIOS INFORMÁTICOS

Artículo 31.. El personal de el Departamento de Informatica realizará periódicamente revisiones de hardware y software del activo informático institucional, para dar atención a problemas de obsolescencia y revisiones de licenciamiento. Además, monitoreará los servicios informáticos de red para administrar el uso del recurso de internet y solucionar cualquier problema detectado.



Artículo 32.. El servicio de Internet a través de las redes institucionales se considera una herramienta de trabajo, por lo que todo usuario deberá utilizarlo exclusivamente para apoyo a sus actividades administrativas y operativas en el OOMSAPAL.

Artículo 33.. Todo responsable de área puede solicitar la restricción total o parcial del acceso a Internet de los equipos de cómputo asignados al personal a su cargo, considerando las funciones laborales que éstos realizan.

Artículo 34.. Todo usuario que descargue información y archivos de Internet mediante el navegador web u otro medio debe evitar descargar archivos de páginas de internet de dudosa procedencia, que pongan en riesgo la información del equipo de cómputo de la persona, e incluso del Organismo, derivado de virus o software malicioso.

CAPÍTULO IX DEL SISTEMA DE VIDEOVIGILANCIA

Artículo 35.. El OOMSAPAL podrá contar con un sistema de videovigilancia (circuito cerrado de cámaras) instalado en sus instalaciones, plantas, pozos, oficinas administrativas y demás inmuebles del Organismo, con el objeto de salvaguardar la integridad de las personas, proteger los activos informáticos y de infraestructura hidráulica, y reforzar la seguridad física de sus instalaciones. La administración, operación y mantenimiento del sistema de videovigilancia será responsabilidad de el Departamento de Informatica, en coordinación con la unidad administrativa que corresponda.

Artículo 36.. Las grabaciones generadas por el sistema de videovigilancia deberán contar con un resguardo de respaldo en la nube, mediante un servicio contratado o autorizado por el Departamento de Informatica, que garantice lo siguiente:

- Cifrado de la información durante su transmisión y almacenamiento en la nube.
- Control de acceso mediante cuentas individuales, contraseñas seguras y, en la medida de lo posible, autenticación de dos factores.
- Definición de un periodo de retención de las grabaciones, conforme a las necesidades operativas y a la normatividad aplicable en materia de protección de datos personales.
- Registro (bitácora) de los accesos y descargas realizadas sobre las grabaciones almacenadas en la nube.

Artículo 37.. El equipo que conforma el sistema de videovigilancia, incluyendo cámaras, grabadores de video (DVR/NVR), servidores de respaldo, switches y demás equipo asociado, es considerado infraestructura crítica del Organismo y deberá contar con las siguientes medidas de protección:

- Instalación en un área de acceso restringido, bajo llave o control de acceso, exclusivo para personal autorizado de el Departamento de Informatica.
- Conexión a través de una red eléctrica regulada y, de ser posible, respaldada con sistemas de alimentación ininterrumpida (UPS), a fin de evitar pérdida de información por fallas en el suministro eléctrico.



- Mantenimiento preventivo y revisiones periódicas a cargo de el Departamento de Informatica, a efecto de verificar el correcto funcionamiento de cámaras, grabadores y enlaces de comunicación.
- Protección mediante contraseñas seguras y, en su caso, segmentación de red, para evitar accesos no autorizados al equipo de videovigilancia desde la red institucional o desde Internet.

Artículo 38.. El acceso a las imágenes y grabaciones del sistema de videovigilancia, ya sea en vivo o almacenadas localmente o en la nube, queda reservado exclusivamente al personal autorizado por el Departamento de Informatica o por la Dirección General, y deberá utilizarse única y exclusivamente para fines de seguridad, supervisión operativa o atención de incidentes, quedando prohibido su uso para fines distintos, así como su copia, divulgación, distribución o publicación, total o parcial, en redes sociales o cualquier otro medio, sin autorización expresa de la Dirección General.

Artículo 39.. El mal uso de las grabaciones del sistema de videovigilancia, la divulgación no autorizada de las mismas, el acceso indebido al equipo de cámaras o a los respaldos en la nube, así como la falta de cuidado que ponga en riesgo la integridad, disponibilidad o confidencialidad de dicha información, será motivo de responsabilidad administrativa para la persona involucrada, en términos del CAPÍTULO XI de los presentes Lineamientos y demás disposiciones legales aplicables, con independencia de las responsabilidades civiles o penales a que haya lugar.

CAPÍTULO X MARCO JURÍDICO APLICABLE

Artículo 40.. Los presentes Lineamientos se emiten y deberán interpretarse y aplicarse en concordancia con el siguiente marco jurídico, sin perjuicio de las demás disposiciones legales aplicables y de las reformas o adiciones que en su caso se realicen:

- Constitución Política de los Estados Unidos Mexicanos, particularmente sus artículos 6º y 16.
- Constitución Política del Estado Libre y Soberano de Baja California Sur, particularmente su artículo 13.
- Ley General de Transparencia y Acceso a la Información Pública.
- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
- Ley de Transparencia y Acceso a la Información Pública del Estado de Baja California Sur.
- Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Baja California Sur.
- Ley de Aguas del Estado de Baja California Sur y demás disposiciones aplicables a los organismos operadores municipales de agua potable, alcantarillado y saneamiento.
- Ley Orgánica del Gobierno Municipal del Estado de Baja California Sur.
- Ley de Gobierno Municipal y demás reglamentos municipales de Loreto, Baja California Sur, aplicables en materia administrativa y de bienes municipales.



- Ley General de Responsabilidades Administrativas y la Ley de Responsabilidades Administrativas del Estado de Baja California Sur.
- Ley General de Archivos y la legislación estatal en materia de archivos aplicable al Estado de Baja California Sur.
- Reglamento Interior y demás normatividad interna del OOMSAPAL.

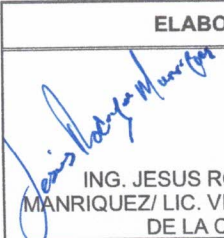
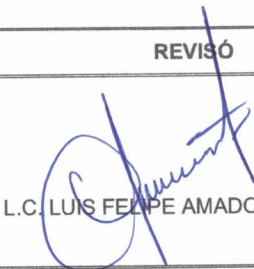
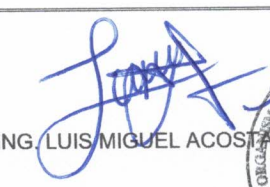
Lo no previsto en los presentes Lineamientos será resuelto por la Dirección General del OOMSAPAL, en coordinación con el Departamento de Informática y el área jurídica del Organismo, atendiendo en todo momento a los principios de máxima publicidad, protección de datos personales y seguridad de la información.

CAPÍTULO XI DISPOSICIONES FINALES

Artículo 41.. El incumplimiento de los presentes Lineamientos por parte del personal del OOMSAPAL podrá dar lugar a la aplicación de las medidas administrativas y, en su caso, a la instauración de los procedimientos de responsabilidad administrativa que correspondan, conforme a la Ley de Responsabilidades Administrativas del Estado de Baja California Sur y demás disposiciones aplicables, con independencia de las responsabilidades civiles o penales a que haya lugar.

Artículo 42.. Los presentes Lineamientos entrarán en vigor al día siguiente de su publicación o difusión interna dentro del OOMSAPAL, y permanecerán vigentes hasta que sean modificados, sustituidos o abrogados por la autoridad competente del Organismo.

01 de abril de 2026, Loreto, Baja California Sur.

ELABORÓ	REVISÓ	AUTORIZÓ
 ING. JESUS RODRIGUEZ MANRIQUEZ/ LIC. VICENTE BENITEZ DE LA CRUZ	 L.C. LUIS FELIPE AMADOR ESTRADA.	 ING. LUIS MIGUEL ACOSTA ACOSTA
JEFE DE INFORMATICA/ORGANO INTERNO DE CONTROL	DIRECTOR DE ADMINISTRACION Y FINANZAS	DIRECTOR GENERAL

