DOCUMENTO DE SEGURIDAD DE DATOS PERSONALES
DEL FIDEICOMISO DE TURISMO DE LOS CABOS (FITURCA)

En Los Cabos Baja California Sur, enero de 2025.

1. PRESENTACIÓN.

El derecho de toda persona a la protección de sus datos personales, así como, el acceso, rectificación, cancelación, oposición y protección de los mismos, se establece en el artículo 13, apartado B, de la Constitución Política del Estado de Baja California Sur, los cuales serán garantizados por el Estado conforme a los principios establecidos en los artículos 6º y 16º de la Constitución Política de los Estados Unidos Mexicanos, esta Constitución local y las leyes que de ellas emanen.

El principio de máxima publicidad constituye el eje rector de la interpretación y aplicación de este derecho. En consecuencia, toda información en posesión de las autoridades, entidades, órganos y organismos de los poderes Ejecutivo, Legislativo y Judicial, de los ayuntamientos, de los órganos constitucionales autónomos, de los partidos políticos, fideicomisos, fondos públicos, así como de cualquier persona física, moral o sindicato que reciba o ejerza recursos públicos o realice actos de autoridad, se presume pública, y sólo podrá ser reservada temporalmente por razones de interés público o de seguridad pública, en los términos que establezcan las leyes aplicables.

Por otra parte, la información relativa a la vida privada y los datos personales debe objeto de protección conforme a los términos y excepciones que dispongan las leyes. Toda persona, sin necesidad de acreditar interés alguno ni justificar el uso de la información, tendrá acceso gratuito a los datos públicos y a los suyos propios, pudiendo solicitar su rectificación, cancelación, oposición y protección en los términos legales aplicables.

Las autoridades garantes, como el Fideicomiso de Turismo de Los Cabos, deben de actuar bajo los principios de certeza, congruencia, documentación, excepcionalidad, exhaustividad, legalidad, independencia, imparcialidad, eficacia, objetividad, profesionalismo, transparencia y máxima publicidad.

Asimismo, el Fideicomiso de Turismo de Los Cabos como sujeto obligado deberá organizar, preservar y actualizar sus archivos administrativos, asegurando la publicación electrónica de la información completa y vigente relativa a sus indicadores de gestión y al ejercicio de los recursos públicos.

Por ende, en cumplimiento de los artículos 30 al 34 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Baja California Sur (LPDPPSOEBCS), el Fideicomiso de Turismo de Los Cabos (FITURCA) establece el presente Documento de Seguridad, el cual describe las medidas administrativas, físicas y técnicas implementadas para garantizar la confidencialidad, integridad y disponibilidad de los datos personales bajo su resguardo.

2. PRINCIPIOS RECTORES Y DEBERES.

I. PRINCIPIOS RECTORES.

FITURCA observará los siguientes principios en todo tratamiento de datos personales:

1. **Legalidad:** El tratamiento de los datos personales deberá efectuarse con fundamento en una facultad expresa derivada de la normatividad aplicable, observando los límites establecidos en las leyes.

2. **Finalidad:** Los datos personales sólo podrán ser tratados para fines determinados, explícitos y legítimos relacionados con las atribuciones institucionales de FITURCA.

3. **Consentimiento:** El tratamiento de datos personales requerirá, cuando proceda, el consentimiento libre, específico e informado del titular, salvo las excepciones previstas en la ley.

4. **Calidad:** La información deberá ser exacta, completa, pertinente, actualizada y necesaria respecto de la finalidad que justifica su tratamiento.

5. **Proporcionalidad:** El tratamiento se limitará a los datos personales que resulten estrictamente necesarios para el cumplimiento de las atribuciones institucionales.

6. **Información:** El titular deberá ser informado sobre la existencia y finalidad del tratamiento, los responsables, los mecanismos para ejercer sus derechos ARCO y las transferencias que se realicen.

7. **Responsabilidad:** FITURCA adoptará medidas efectivas, verificables y proactivas para garantizar el cumplimiento de los principios, deberes y obligaciones previstos en la normativa aplicable.

II. DEBERES.

1. **Deber de confidencialidad.** Todo servidor público o persona que intervenga en el tratamiento de datos personales deberá guardar confidencialidad y secreto respecto de la información a la que tenga acceso, incluso después de finalizar su relación laboral o contractual con FITURCA.

2. **Deber de seguridad.** FITURCA implementará controles y medidas de seguridad administrativas, físicas y técnicas proporcionales al riesgo y sensibilidad de los datos personales tratados, con el fin de evitar su alteración, pérdida, acceso o divulgación no autorizada.

3. OBJETO Y ALCANCE.

I. OBJETO.

El presente Documento de Seguridad de Datos Personales del Fideicomiso de Turismo de Los Cabos (FITURCA), tiene por objeto establecer las medidas, políticas, procedimientos, controles y mecanismos técnicos y administrativos que garanticen la protección, integridad, confidencialidad, disponibilidad y licitud del tratamiento de los datos personales en posesión de esta entidad pública.

Este documento se formula en cumplimiento de los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de datos personales, previstos en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, así como, de los principios de transparencia, máxima publicidad y rendición de cuentas establecidos en la Constitución Política del Estado de Baja California Sur.

En ese sentido, su propósito es asegurar que el tratamiento de los datos personales que realiza FITURCA, ya sea en medios físicos, digitales o electrónicos, se efectúe de manera lícita, controlada y segura, evitando su alteración, pérdida, destrucción, uso, acceso o divulgación no autorizados, y garantizando en todo momento el derecho de los titulares al acceso, rectificación, cancelación, oposición y protección (derechos ARCO) de sus datos personales.

Asimismo, el Documento de Seguridad constituye un instrumento de gestión institucional que permite a FITURCA cumplir con su obligación de proteger los datos personales derivados de sus funciones de promoción turística, vinculación institucional, gestión administrativa, cooperación con el sector privado y ejecución de recursos públicos, en los términos que marca la legislación aplicable.

II. ALCANCE.

El presente Documento de Seguridad tiene un alcance integral y es de observancia obligatoria para todo el personal adscrito al Fideicomiso de Turismo de Los Cabos (FITURCA), incluyendo:

- Servidores públicos de confianza o eventuales;
- Prestadores de servicios profesionales, asesores y contratistas que, por la naturaleza de sus funciones, tengan acceso o intervención en el tratamiento de datos personales;
- Terceros receptores de datos personales, cuando el tratamiento derive de convenios de colaboración, contratos, alianzas estratégicas o cualquier otro instrumento jurídico que implique transferencia o cesión de información.

Este documento aplica a todas las bases de datos que contengan información personal en posesión de FITURCA, sin importar su formato, medio o sistema de almacenamiento, incluyendo:

- Bases de datos electrónicas administradas en sistemas institucionales, servidores locales o servicios en la nube;
- Expedientes físicos o digitales generados en el ejercicio de las funciones sustantivas y administrativas del Fideicomiso;
- Plataformas electrónicas de registro o participación utilizadas para eventos, ferias, campañas de promoción, encuestas, alianzas o convenios;
- Sistemas de videovigilancia o control de acceso, en los términos de las disposiciones aplicables.

El cumplimiento de este documento implica la aplicación de medidas de seguridad administrativas, físicas y técnicas, en niveles acordes con la sensibilidad de los datos tratados, y la observancia de los protocolos de actuación establecidos para la gestión de incidentes de seguridad, la respuesta ante vulneraciones y la notificación a las autoridades competentes.

De igual forma, el alcance del presente instrumento comprende la implementación y seguimiento continuo de acciones de capacitación, concientización y mejora orientadas a fortalecer la cultura institucional de transparencia responsable y protección de datos personales, asegurando la armonía entre el derecho a la información pública y el derecho a la privacidad de las personas.

4. SISTEMA DE GESTIÓN DE DATOS PERSONALES.

I. MEDIDAS DE SEGURIDAD ADMINISTRATIVAS, FÍSICAS Y TÉCNICAS.

Medidas administrativas.

I. Designar a un Responsable de Protección de Datos Personales, quien fungirá como enlace con el Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de Baja California Sur (ITAIP-BCS).
II. Establecer perfiles de acceso y niveles de autorización al interior de cada unidad administrativa.
III. Integrar y mantener actualizado un inventario de bases de datos personales en posesión de FITURCA.
IV. Implementar programas de capacitación y concientización para todo el personal con acceso a información personal.
V. Establecer protocolos de gestión y conservación de archivos que aseguren la trazabilidad y control documental.

Medidas físicas.

I. Asegurar las instalaciones donde se resguarden datos personales mediante controles de acceso, videovigilancia y dispositivos de seguridad.
II. Contar con espacios físicos y mobiliario cerrado para el archivo y custodia de expedientes.
III. Garantizar la disposición final segura de los soportes que contengan datos personales, incluyendo su destrucción o reciclaje bajo métodos certificados.

Medidas técnicas.

I. Implementar sistemas informáticos seguros, con controles de autenticación, contraseñas robustas y registros de acceso.
II. Aplicar protocolos de respaldo y recuperación de información en caso de contingencia o fallo técnico.
III. Utilizar cifrado y anonimización de datos personales cuando su transferencia o almacenamiento lo requiera.
IV. Asegurar que las transferencias de datos a terceros se realicen únicamente con instrumentos jurídicos válidos y bajo condiciones de seguridad verificables.

II. PROCEDIMIENTOS DE ATENCIÓN A INCIDENTES Y DERECHOS ARCO.

Incidentes de seguridad.

En caso de detectar una vulneración o incidente que comprometa la seguridad de los datos personales, FITURCA deberá:

- **I.** Registrar el incidente en el sistema institucional de control y notificar al Responsable de Datos Personales;
- **II.** Adoptar medidas inmediatas para contener el riesgo y evitar mayores afectaciones;
- **III.** Evaluar el impacto sobre los derechos de los titulares;
- **IV.** Notificar al ITAIP-BCS y al titular afectado en los términos previstos por la ley.

Ejercicio de derechos ARCO.

FITURCA garantizará que toda persona pueda ejercer los derechos de Acceso, Rectificación, Cancelación y Oposición (ARCO) respecto de sus datos personales, mediante un procedimiento gratuito, expedito y sin discriminación, conforme a los lineamientos del Sistema Nacional de Transparencia y las disposiciones aplicables.

Registro y seguimiento.

El Responsable de Protección de Datos llevará un registro sistemático de las solicitudes ARCO y de los incidentes de seguridad, asegurando su seguimiento y resolución conforme a los plazos legales.

III. SUPERVISIÓN, VIGILANCIA Y SANCIONES.

Supervisión y evaluación.

FITURCA establecerá mecanismos internos de revisión y supervisión periódica del cumplimiento de este Documento de Seguridad, documentando los resultados y corrigiendo cualquier deficiencia detectada.

Responsabilidad administrativa.

El incumplimiento de las disposiciones contenidas en el presente documento será sancionado conforme a lo dispuesto en la legislación estatal y federal en materia de responsabilidades administrativas y protección de datos personales.

IV. VIGENCIA Y ACTUALIZACIÓN.

Vigencia.

El presente Documento de Seguridad entrará en vigor a partir de su aprobación por el Director General del Fideicomiso de Turismo de Los Cabos y permanecerá vigente hasta su modificación o actualización formal por parte del Comité de Transparencia de FITURCA, asimismo, deberá conservarse como evidencia del cumplimiento de los artículos 30 al 34 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Baja California Sur.

Actualización.

Este instrumento deberá revisarse y actualizarse al menos una vez cada doce meses o cuando ocurran cambios sustanciales en la normatividad, estructuras administrativas, sistemas informáticos o procesos de tratamiento de datos personales.

5. DISPOSICIONES FINALES.

FITURCA reafirma su compromiso con los principios de **transparencia, máxima publicidad y rendición de cuentas**, garantizando simultáneamente la **protección de la privacidad y la dignidad de las personas** cuyos datos personales sean tratados. Este documento constituye un componente esencial del **Sistema Institucional de Transparencia y Protección de Datos Personales** del Fideicomiso de Turismo de Los Cabos.

Así lo acordó y firma Rodrigo Esponda Cascajares, Director General del Fideicomiso de Turismo de Los Cabos.

ANEXO TÉCNICO

I. OBJETO DEL ANEXO TÉCNICO.

El presente Anexo Técnico tiene por objeto establecer los mecanismos, metodologías y herramientas operativas que permitan a FITURCA implementar, supervisar y evaluar las medidas administrativas, físicas y técnicas descritas en el cuerpo normativo del Documento de Seguridad, garantizando la protección integral de los datos personales bajo su custodia.

II. CLASIFICACIÓN Y NIVEL DE SENSIBILIDAD DE LOS DATOS PERSONALES.

De conformidad con el artículo 3, fracción X, de la LGPDPPSO, se consideran datos personales sensibles aquellos que se refieren a la esfera más íntima del titular, o cuya utilización indebida pueda generar discriminación o un riesgo grave.

Para efectos de gestión de seguridad, FITURCA clasifica los datos personales conforme al nivel de riesgo asociado a su tratamiento.

Nivel de Sensibilidad	Tipo de Dato Personal	Ejemplo	Medidas de Seguridad Requeridas
Bajo	Identificativos básicos	Nombre, puesto, correo institucional	Contraseñas y accesos restringidos por perfil
Medio	Laborales y de contacto	Teléfono personal, domicilio laboral, historial de asistencia a eventos	Control de accesos, respaldo cifrado y registro de acceso
Alto (Sensibles)	Datos financieros, biométricos, médicos o ideológicos	Información bancaria, huellas, imágenes, condiciones de salud	Cifrado, anonimización, almacenamiento restringido, supervisión del Responsable de Datos Personales

III. MATRIZ DE RIESGOS EN EL TRATAMIENTO DE DATOS PERSONALES.

Esta matriz identifica los riesgos potenciales, su probabilidad, impacto, y las acciones de mitigación que FITURCA debe adoptar:

Riesgo Identificado	Probabilidad	Impacto	Medidas Preventivas	Medidas Correctivas
Acceso no autorizado a bases de datos	Media	Alto	Control de usuarios, autenticación de dos factores	Bloqueo inmediato de cuentas y auditoría de accesos
Pérdida de información por falla técnica	Media	Alto	Respaldo semanal en nube segura	Restauración desde respaldo y registro de incidente

Divulgación indebida por error humano	Alta	Medio	Capacitación continua y firma de compromisos de confidencialidad	Notificación al ITAI-BCS y corrección de procedimiento
Robo o extravío de dispositivos	Media	Alto	Asignación de equipos institucionales y cifrado de disco	Reporte al área jurídica y desactivación remota
Ataques informáticos (*malware*, *phishing*, *ransomware*)	Alta	Muy alto	Antivirus, firewall y protocolos de actualización	Contención inmediata, reporte técnico y restablecimiento controlado

IV. RESPONSABLES Y PERFILES DE ACCESO.

Para garantizar la trazabilidad y el control de la información, se establecen los siguientes niveles de acceso:

Nivel de Acceso	Perfil	Facultades	Responsabilidades
Nivel 1	Dirección General	Acceso total a sistemas y expedientes	Supervisar cumplimiento normativo y aprobar medidas de seguridad
Nivel 2	Responsable de Protección de Datos Personales	Acceso a bases de datos y reportes de incidentes	Coordinar la implementación del Documento de Seguridad
Nivel 3	Unidades Administrativas	Acceso limitado a la información necesaria para su función	Cumplir con medidas de seguridad y confidencialidad
Nivel 4	Personal Operativo o Contratistas	Acceso restringido o supervisado	Manejar datos conforme a instrucciones y políticas internas

V. PROTOCOLOS DE GESTIÓN DE INCIDENTES DE SEGURIDAD.

a) **Detección:** Cualquier servidor público que advierta una vulneración o riesgo deberá informar de inmediato al Responsable de Protección de Datos Personales.
b) **Evaluación:** El Responsable determinará la naturaleza, alcance e impacto del incidente sobre los derechos de los titulares.
c) **Contención:** Se implementarán medidas inmediatas para detener el daño o fuga de información.
d) **Notificación:**
   - **Interna:** Comunicación al Titular de la Unidad Administrativa correspondiente.
   - **Externa:** Notificación formal al ITAI-BCS sobre la detección del incidente, conforme a la LPDPPSOEBCS.
e) **Registro:** Todo incidente deberá documentarse en la Bitácora de Incidentes de Seguridad, incluyendo causas, consecuencias, medidas adoptadas y fecha de cierre.
f) **Corrección y mejora:** Una vez solventado el incidente, se actualizarán los procedimientos internos para evitar su repetición.

VI. PROCEDIMIENTO DE ATENCIÓN A SOLICITUDES ARCO.

1. **Recepción:** Las solicitudes se presentarán por escrito o a través de medios electrónicos ante la Unidad de Transparencia de FITURCA.
2. **Verificación de identidad:** Se corroborará la identidad del solicitante o su representante legal.
3. **Análisis y respuesta:** La Unidad de Transparencia turnará la solicitud al área competente, que dispondrá de 20 días hábiles para resolver, prorrogables conforme a la ley.
4. **Entrega o negativa fundada:**
    - Si procede, se entregará la información de manera segura, sin poner en riesgo datos de terceros.
    - Si no procede, se emitirá resolución fundada y motivada conforme a los supuestos de excepción de la ley.
5. **Registro:** Se documentará cada solicitud en el Sistema de Control de Solicitudes ARCO, incluyendo fecha, tipo de derecho ejercido y resolución.

VII. MEDIDAS DE SEGURIDAD INFORMÁTICA Y DE INFRAESTRUCTURA.

- Uso obligatorio de contraseñas robustas (mínimo 8 caracteres, con letras, números y símbolos).
- Cambio periódico de contraseñas.
- Actualización continua de *software* y sistemas de seguridad.
- Cifrado de discos duros y dispositivos móviles.
- Uso de redes seguras y *VPN* para accesos remotos.
- Respaldo automático de información crítica en servidores institucionales y nube segura.
- Monitoreo permanente de logs de acceso a sistemas.

VIII. PLAN DE CAPACITACIÓN Y CONCIENTIZACIÓN.

El Responsable de Protección de Datos Personales coordinará un Programa de Capacitación cuando sea necesario, que incluirá:

- Sensibilización sobre derechos ARCO y principios de protección de datos personales;
- Buenas prácticas en manejo de información digital y documental;
- Protocolos de prevención de incidentes de seguridad;
- Actualización sobre cambios legislativos o lineamientos del INAI o ITAI-BCS.

IX. SEGUIMIENTO, AUDITORÍA Y MEJORA CONTINUA.

1. **Evaluación interna anual** del cumplimiento de las medidas de seguridad, a cargo del Responsable de Datos Personales.
2. **Informe de resultados** al Comité de Transparencia de FITURCA, con recomendaciones y acciones correctivas.

3. **Actualización del Documento de Seguridad y del Anexo Técnico**, cuando:
    - Se modifiquen los procesos institucionales o tecnológicos;
    - Se detecten vulneraciones relevantes; o
    - Se emitan nuevas disposiciones normativas.

X. DISPOSICIONES FINALES.

El presente Anexo Técnico forma parte integrante del Documento de Seguridad de Datos Personales del Fideicomiso de Turismo de Los Cabos (FITURCA) y deberá publicarse en versión pública en el portal institucional, conforme a los principios de máxima publicidad y rendición de cuentas.

FITURCA reitera su compromiso con la protección efectiva de los datos personales, la seguridad de la información pública, y la observancia de los estándares del Sistema Nacional de Transparencia.