



**BAJA
CALIFORNIA**
GOBIERNO DEL ESTADO

INSTITUTO DE CULTURA DE BAJA CALIFORNIA

DOCUMENTO DE SEGURIDAD.

RESPONSABLE DE SU ELABORACIÓN:
OFICIAL DE PROTECCIÓN DE DATOS PERSONALES Y
TITULARES DE LAS UNIDADES ADMINISTRATIVAS.

MEXICALI BAJA CALIFORNIA A 17 DE NOVIEMBRE DE 2021.



ÍNDICE.

Contenido

ÍNDICE.....	2
INTRODUCCIÓN.....	3
GLOSARIO DE TERMINOS.....	4
INVENTARIO Y CATÁLOGO DE DATOS PERSONALES Y DE LOS SISTEMAS DE TRATAMIENTO.	6
NIVEL DE SEGURIDAD DE LOS DATOS PERSONALES A LOS QUE SE LES DA TRATAMIENTO POR EL ICBC.....	8
TRANSFERENCIAS DE LOS DATOS PERSONALES.	9
LAS FUNCIONES Y OBLIGACIONES DE LAS PERSONAS QUE TRATEN DATOS PERSONALES.....	9
REGISTRO DE INCIDENCIAS.	10
IDENTIFICACIÓN Y AUTENTIFICACIÓN.....	10
ANÁLISIS DE RIESGOS.....	10
ANALISIS DE BRECHA.....	11
PLAN DE TRABAJO.....	11
LOS MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD.	12
PROGRAMA DE CAPACITACIÓN.....	13



INTRODUCCIÓN.

En el presente documento se detallan las medidas de seguridad administrativas, físicas y técnicas con las que contará en el Instituto de Cultura de Baja California para garantizar la debida protección de los datos personales a los que se les da tratamiento en las direcciones que los manejan.

Con este documento de seguridad se da cumplimiento lo establecido en el Artículo 4, fracción XII y el Artículo 18 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Baja California, publicada en el Periódico Oficial NO 38, Sección III, de fecha 18 de agosto de 2017, Tomo CXXIV.

Dado en la ciudad de Mexicali, B.C., 17 de noviembre de 2021.



GLOSARIO DE TERMINOS.

- **Base de datos:** Conjunto ordenado de datos personales que estén en posesión del responsable, ya sea en formato escrito, impreso, digital, sonoro, visual, electrónico, informático u holográfico, referentes a una persona física o moral identificada o identificable, condicionados a criterios determinados, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.
- **Datos personales:** Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo, concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información.
- **Derechos ARCO-P:** Los derechos de Acceso, Rectificación, Cancelación, Oposición y Portabilidad al tratamiento de datos personales.
- **Documento de seguridad:** Instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee.
- **ICBC:** Instituto de Cultura de Baja California.
- **Inventario de datos personales:** Lista ordenada y detallada que posea el responsable o encargado, de cualquier información numérica, alfabética, gráfica, fotográfica, acústica; o de cualquier tipo, concerniente a una persona física identificada o identificable.
- **Ley:** Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Baja California.
- **Medidas de seguridad:** Conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger los datos personales.
- **Medidas de seguridad administrativa:** Políticas, acciones y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación, clasificación y borrado seguro de la información, así como la sensibilización y capacitación del personal, en materia de protección de datos personales.



- **Medidas de seguridad físicas:** Conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento como prevenir el acceso no autorizado al perímetro de la organización, sus instalaciones físicas, áreas críticas, recursos de información.
- **Titular:** La persona física a quien corresponden los datos personales.
- **Tratamiento:** Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionadas con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, publicación, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia a disposición de datos personales.



INVENTARIO Y CATÁLOGO DE DATOS PERSONALES Y DE LOS SISTEMAS DE TRATAMIENTO.

A continuación se describen las categorías de datos personales con los que cuenta el ICBC, categorizado por personas de quienes se obtienen los datos personales:

DATOS DE IDENTIFICACIÓN Y CONTACTO			
Personal	Proveedores	Colaboradores/Artistas	Solicitantes
Nombre completo, Estado civil, RFC, CURP, Lugar de nacimiento, Fecha de nacimiento, Nacionalidad, Domicilio, Teléfono particular, Teléfono celular, Correo electrónico, Firma autógrafa, Edad, Fotografía, Referencias personales.	Nombre completo, RFC, CURP (en caso de ser física) INE (en caso de ser física) Acta constitutiva (cuando es persona moral) Teléfono del negocio, Teléfono celular, Correo electrónico, Firma autógrafa, Comprobante de domicilio, Referencias personales.	Nombre completo, RFC, Nacionalidad; en caso de ser de nacionalidad extranjera, deberá acreditar su estancia en el país y contar con su visa de trabajo. Domicilio, Teléfono particular, Teléfono celular, Correo electrónico, Firma autógrafa. En el caso de asistentes a capacitaciones y/o eventos solo se solicitan nombre, correo y teléfono.	Nombre (pseudónimo) Correo electrónico, en caso de solicitud de Derechos ARCO-P deberá acreditar la Titularidad con su INE.

DATOS BIOMÉTRICOS			
Personal	Proveedores	Colaboradores/Artistas	Solicitantes
Huella dactilar	NINGUNO	NINGUNO	NINGUNO

DATOS LABORALES			
Personal	Proveedores	Colaboradores/Artistas	Solicitantes
Puesto o cargo que desempeña, Domicilio de trabajo, Correo electrónico institucional, Teléfono de oficina, Referencias laborales, Información generada durante los procedimientos de reclutamiento, selección y contratación, Experiencia laboral, Capacitación laboral.	Puesto o cargo que desempeña, Domicilio del negocio, Correo electrónico oficial, Teléfono de oficina.	En el caso de convenios de colaboración se solicita su reseña curricular. En el caso de participación en convocatorias se solicitarán documentos que acrediten su experiencia laboral	NINGUNO



DATOS ACADÉMICOS			
Personal	Proveedores	Colaboradores/Artistas	Solicitantes
De acuerdo al puesto específico a desempeñar se le podrá solicitar alguno de los siguientes: Trayectoria educativa, Título, Cédula profesional, Certificados, Constancias, Reconocimientos.	NINGUNO	NINGUNO En el caso de participación en convocatorias se solicitarán documentos que acrediten su trayectoria académica.	NINGUNO

DATOS PATRIMONIALES Y/O FINANCIEROS			
Personal	Proveedores	Colaboradores/Artistas	Solicitantes
Ingresos, Egresos, Cuenta bancaria (nómina), Seguro de vida.	NINGUNO	Solo en caso de que el pago por sus servicios, sea a través de transferencia se solicitará número de cuenta para la realización del pago.	NINGUNO

DATOS LEGALES			
Personal	Proveedores	Colaboradores/Artistas	Solicitantes
Carta de no antecedentes penales. Certificado de no inhabilitación del servicio público.	NINGUNO	En el caso de concursar en alguna convocatoria de recurso federal, deberá presentar constancia de no adeudo con algún programa anterior.	NINGUNO



DATOS DE SALUD			
Personal	Proveedores	Colaboradores/Artistas	Solicitantes
Certificado médico.	NINGUNO	NINGUNO	NINGUNO

DATOS PERSONALES DE NATURALEZA PÚBLICA			
Personal	Proveedores	Colaboradores/Artistas	Solicitantes
Datos que por mandato legal son de acceso público.	NINGUNO	Los que se establezcan en las Convocatorias, siendo generalmente: Nombre completo, Nombre de su proyecto/trabajo/etc. Municipio al que pertenece.	NINGUNO

Los datos personales se recaban por medio de documentos presentados y/o por el llenado de formularios físicos y/o electrónicos por los titulares de los datos personales.

NIVEL DE SEGURIDAD DE LOS DATOS PERSONALES A LOS QUE SE LES DA TRATAMIENTO POR EL ICBC.

Para garantizar la seguridad en los datos personales y en las bases de datos personales, físicas o electrónicas, donde se concentran los mismos, las medidas de seguridad que se implementan corresponden a un nivel de seguridad **MEDIO**, siempre garantizando la confidencialidad, integridad y disponibilidad de los mismos a los titulares, de acuerdo a lo establecido en la Ley.



TRANSFERENCIAS DE LOS DATOS PERSONALES.

Toda transferencia de datos personales, sea nacional o internacional, se encuentra sujeta al consentimiento de su titular, salvo las excepciones previstas en la Ley.

LAS FUNCIONES Y OBLIGACIONES DE LAS PERSONAS QUE TRATEN DATOS PERSONALES.

Las Direcciones, Coordinaciones y Unidades encargadas de tratar datos personales son las siguientes:

- Dirección General.
- Unidad Jurídica.
- Coordinación de Proyectos Culturales Comunitarios.
- Órgano Interno de Control.
- Unidad de Planeación, Evaluación y Transparencia.
- Coordinación General de Patrimonio y Difusión Cultural.
- Dirección de Patrimonio y Culturas Populares.
- Dirección de Artes Escénicas.
- Dirección de Difusión Cultural y Fomento Artístico.
- Dirección de Museos y Galerías.
- Coordinación General de Educación Artística y Fomento a la Lectura.
- Dirección Editorial y de Fomento a la Lectura.
- Dirección de Académica y de Talentos Artísticos.
- Centros Estatales de las Artes (Mexicali, Tecate, Tijuana, Playas de Rosarito, Ensenada)
- Delegación Zona Costa.
- Subdelegación San Quintín.
- Dirección de Promoción y Vinculación.
- Dirección de Administración.

Los titulares de las Unidades Administrativas anteriormente mencionadas, tienen como funciones y obligaciones las siguientes:

- a) Prevenir que el acceso a las bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados.
- b) Garantizar la debida protección de los datos personales, conforme a la Ley y las demás disposiciones aplicables en la materia.
- c) Implementar medidas de seguridad físicas, técnicas y administrativas convenientes para el tratamiento diario de los datos personales.
- d) Garantizar la confidencialidad de los datos personales derivada de los procedimientos que tienen a su cargo.
- e) Conocer y aplicar las acciones derivadas de este Documento de Seguridad.
- f) En caso de que se presente algún incidente de vulneración de seguridad de los datos personales y/o de los sistemas de tratamiento de los mismos,



- informar dicho incidente a la Unidad de Planeación, Evaluación y Transparencia del ICBC y llevar el registro de los hechos.
- g) Atender los mecanismos para asegurar que los datos personales a los que tengan acceso en el ejercicio de sus atribuciones no se difundan, distribuyan o comercialicen.

REGISTRO DE INCIDENCIAS.

Las incidencias con datos personales que se produzcan vulnerarán la debida protección de los mismos, por lo tanto, es necesario que en las Unidades Administrativas del ICBC en donde se de tratamiento a datos personales lleven a cabo un registro de las incidencias que comprometen la seguridad de los datos.

El registro de incidencias deberá contener; por lo menos, la fecha de la incidencia, el tipo, descripción, la persona quien la registra, persona a quien se la comunica y la o las consecuencias que tendrá esa incidencia.

El personal del ICBC que trate datos personales deberá de contar con el registro de incidencias, ya que quien identifique la incidencia será el encargado de registrarla y notificar a su superior inmediato, quien a su vez se encargará de notificar a la o las personas afectadas para que éste tome las precauciones debidas en caso de uso inadecuado de la información.

IDENTIFICACIÓN Y AUTENTIFICACIÓN.

La Dirección de Administración a través del personal del área de Tecnologías de la información será quien administre las altas y bajas de correos electrónicos oficiales del personal del ICBC, así como las sesiones en los equipos de cómputo, asignando usuarios y contraseñas, siendo aleatorias y en cada movimiento del personal; cualquiera que sea el caso, se modificaran de forma inmediata.

La reserva y confidencialidad de estas contraseñas queda bajo la responsabilidad de la persona a la que se le asignó la cuenta de usuario y por ningún motivo las cuentas y contraseñas de los usuarios de correos o de equipos de cómputo se podrán compartir o transferir.

ANÁLISIS DE RIESGOS.

Los datos personales a los que los servidores públicos del ICBC tienen acceso en el ejercicio de sus atribuciones y dan tratamiento a los datos personales; se resguardan de manera física y electrónica, según las necesidades de la actividad, además se advierten como las vulneraciones comunes las siguientes:

- a) Extravío o copia no autorizada.
- b) Destrucción no autorizada.
- c) Daños por situaciones fortuitas.



ANÁLISIS DE BRECHA.

Las medidas de seguridad existentes y efectivas para la protección de datos personales con las que actualmente cuenta el ICBC, son las siguientes:

1. **Medidas de seguridad:** La información que contiene datos personales se resguarda en una ubicación que cuenta con medidas de seguridad como cámaras de seguridad, archiveros específicos para su resguardo y el uso de cerraduras para su acceso.
2. **Medidas de control:** Medidas de carácter administrativo encaminadas a contar con un registro físico de los servidores públicos que tienen acceso a datos personales, así como de los datos personales contenidos en los documentos.
3. **Medidas legales:** Cuando se lleva a cabo la transferencia de datos personales entre Sujetos Obligados, se realiza el apercibimiento en cuanto al trato que se le deberá dar a los mismos, en los términos establecidos en la Ley y demás ordenamientos jurídicos administrativos vigentes en la materia.

Como resultado del análisis de la brecha y fijarla entre las medias de seguridad contra las faltantes y/o nuevas por implementar por parte del ICBC, se han identificado las siguientes:

1. Implementar la gestión de capacitación al personal cursos, talleres, programas o videoconferencias enfocados a la protección de datos personales.
2. Designar a un Oficial de Protección de Datos Personales, tal y como lo establece la Ley.
3. La persona designada como Oficial de Protección de Datos Personales, deberá estar a cargo de la vigilancia del cumplimiento de la política de Protección de Datos Personales de manera continua.
4. Se deben designar deberes y obligaciones respecto a los servidores públicos que intervengan en el uso y protección de datos personales.

PLAN DE TRABAJO.

El plan de trabajo para la protección de los datos personales que el ICBC llevará a cabo será cumplir con el proyecto que se tiene contemplado en la Unidad de Planeación, Evaluación y Transparencia, siendo la Verificación y Capacitación Trimestral en materia de Datos Personales, de la siguiente forma:

1. Canalizar a cada Unidad Administrativa que trate datos personales; una encuesta sobre el estado actual del cumplimiento de las obligaciones en la materia.
2. Implementar recomendaciones de medidas de seguridad físicas, administrativas y técnicas para la protección de los datos personales.
3. Revisar y conformar el documento de seguridad como lo requiere la Ley.
4. Capacitar al menos a cada titular y una persona administrativa-operativa de cada Unidad Administrativa que conforma el ICBC.



LOS MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD.

En el presente documento de seguridad para la protección de datos personales, se detallan las acciones que establecen el mantenimiento de las medidas de seguridad en las cuales de manera general se destaca que el objeto de las mismas es la protección de los datos personales.

Por ello y con la finalidad de mantener un seguimiento y revisión de las medidas de seguridad, se llevarán a cabo las acciones siguientes:

1. La Unidad de Planeación, Evaluación y Transparencia llevará un monitoreo del cumplimiento por parte de los servidores públicos que intervengan en las actividades detalladas en el Plan de Trabajo del presente documento.
2. Se mantendrá actualizado el inventario de datos personales y de los sistemas de tratamiento de los mismos.
3. La Dirección de Administración a través del personal de Tecnologías de la Información mantendrá monitoreados los esquemas de seguridad implementados para la infraestructura de tecnología de la información, comunicaciones y sistemas que permitan garantizar conexiones seguras, tanto al exterior como al interior del ICBC.
4. Para garantizar el cumplimiento de las políticas en materia de protección de datos personales establecidos en el presente documento de seguridad, el mismo se publicará en la página web oficial del ICBC y se enviará por medios electrónicos a los servidores públicos del Instituto.
5. Se llevarán a cabo diversas medidas de seguridad físicas para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento mediante las siguientes actividades:
 - 1) Prevenir el acceso no autorizado al perímetro del lugar en que se resguarden los datos personales en las instalaciones físicas.
 - 2) Prevenir el daño o interferencia a las instalaciones físicas, recursos e información.
 - 3) Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico, que pueda salir de las instalaciones del ICBC.
 - 4) Proveer a los equipos que contienen o almacenas datos personales de un mantenimiento eficaz que asegure su disponibilidad, funcionalidad e integridad.



PROGRAMA DE CAPACITACIÓN.

El Instituto de Cultura de Baja California (ICBC), ha promovido la capacitación de los servidores públicos en materia de protección de datos personales, mediante la gestión de capacitación con la Secretaría de la Honestidad y la Función Pública, con el Órgano Garante en Baja California; Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (ITAIP) , así como con el Instituto Nacional de de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), con la finalidad de adquirir los conocimientos de los aspectos fundamentales de la Ley, garantizando el derecho a la protección de los mismos.

De esta manera durante los años 2019, 2020 y 2021, el ICBC ha capacitado al personal; tal y como se ha descrito en el presente documento en la sección Plan de Trabajo, sobre los temas de:

- 1) El ABC de la Protección de los Datos Personales.
- 2) Atribuciones y funciones del Comité Técnico de Transparencia.
- 3) Test Data: Elaboración de Documentos en su Versión Pública.
- 4) Clasificación, Desclasificación y Prueba de Daño.
- 5) Taller Nacional de Elaboración de Avisos de Privacidad.
- 6) Ética pública.
- 7) Protección de Datos Personales. Inteligencia Artificial y Ciberseguridad.
- 8) Protección de Datos Personales frente al covid-19.
- 9) La Protección de Datos Personales como Eje para Relanzar una Estrategia Nacional de Ciberseguridad.

En este sentido, se busca continuar con la promoción de la capacitación en la materia, a través de los cursos citados e incluir otros más, con el apoyo de la Secretaría de la Honestidad y la Función Pública de Baja California, del Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales de Baja California y del Instituto Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, que permitan ampliar los conocimientos a adquirir por parte de los Servidores Públicos del ICBC, por lo que se continuará en constante comunicación/vinculación con los citados Órganos para tales efectos.