



FORMATO 1

CONCENTRADO

A1 - Tipo de Responsable	Poder Ejecutivo		C1 - Periodo que se informa		2024
B1 - Nombre del Responsable	Sistema de Atención a Niños, Niñas y Adolescentes Farmacodependientes del Estado de Campeche "Vida Nueva"				

D1 - Tipo de atención o respuesta proporcionada	Acceso		Rectificación		Número de solicitudes recibidas según tipo de Derecho		Oposición		Portabilidad	
	Físico	Electrónico	Físico	Electrónico	Físico	Electrónico	Físico	Electrónico	Físico	Electrónico
a) Atendidas dentro de los 20 días <u>sin</u> costo de recuperación	0	0	0	0	0	0	0	0	0	0
b) Atendidas dentro de los 20 días con costo de recuperación	0	0	0	0	0	0	0	0	0	0
c) Atendidas con prórroga de tiempo <u>sin</u> costo de recuperación	0	0	0	0	0	0	0	0	0	0
d) Atendidas con prórroga de tiempo con costo de recuperación	0	0	0	0	0	0	0	0	0	0
e) Fuera del plazo legal	0	0	0	0	0	0	0	0	0	0
f) Inexistencia de los datos personales	0	0	0	0	0	0	0	0	0	0
g) Incompetencia	0	0	0	0	0	0	0	0	0	0
h) Improcedencia	0	0	0	0	0	0	0	0	0	0
i) Reconducidas	0	0	0	0	0	0	0	0	0	0
k) Desechadas por no haberse desahogado la prevención	0	0	0	0	0	0	0	0	0	0
l) Orientadas a trámite o procedimiento específico	0	0	0	0	0	0	0	0	0	0
m) Solicitudes pendientes de respuesta para el periodo 2024	0	0	0	0	0	0	0	0	0	0
n) Total de Solicitudes Previstas	0	0	0	0	0	0	0	0	0	0

E1 - Nombre, cargo y firma de quien lo elaboró	Licda. Diana Angelica Jaramillo Clemente	F1 - Total de solicitudes recibidas ARCO-P	0
Mecanismo de Recepción	Responsable de la Unidad de Transparencia		

* Físico - Documento impreso presentado ante el Responsable.
 * Electrónico - Documento presentado ante el responsable en cualquier medio digital: Correo Electrónico, Página Web, etc., incluida la Plataforma Nacional de Transparencia.

FORMATO 3

ACTIVIDADES

A1 - Nombre del activista	A2 - Nombre del sistema de datos	A3 - Nombre del Responsable	A4 - Descripción de la actividad	A5 - Fecha de inicio	A6 - Fecha de término	A7 - Estado de avance
	Activos de privacidad		<p>1. Sistema de Datos Personales del Expediente Clínico</p> <p>2. Sistema de Datos Personales de Recursos Humanos</p> <p>3. Sistema de Datos Personales de Acceso a la Información Pública</p> <p>4. Sistema de Datos Personales de Proveedores</p>			
			<p>1. Medida de seguridad</p> <p>2. Medida de seguridad física</p> <p>3. Medida de seguridad electrónica</p>			

Indicar si el responsable cuenta con lo siguiente:

C1 - Documento de seguridad	C2 - En caso de responder sí	C3 - Fecha de producción por el Comité de Transparencia
No	No	

1. Medida de seguridad administrativa (especificar)	2. Medida de seguridad física	3. Medida de seguridad electrónica (especificar)	4. Medida de seguridad física	5. Medida de seguridad electrónica (especificar)
1.1 Política y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional	2.1 Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas, recursos e información	3.1 Prevenir que el acceso a las bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados	4.1 Prevenir que el acceso a las bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados	5.1 Prevenir que el acceso a las bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados
1.2 Identificación, clasificación y marcado seguro de la información	2.2 Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la instalación	3.2 Generar un esquema de protecciones para que el usuario no se vea afectado por las acciones de los usuarios no autorizados	4.2 Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la instalación	5.2 Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la instalación
1.3 Sensibilización y capacitación del personal en materia de protección de datos personales	2.3 Prevenir el acceso no autorizado al patrimonio de la instalación, sus instalaciones físicas, áreas críticas, recursos e información	3.3 Realizar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento de software y hardware	4.3 Realizar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento de software y hardware	5.3 Realizar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento de software y hardware
1.4 Otra medida de seguridad administrativa (especificar)	2.4 Prevenir el acceso no autorizado al patrimonio de la instalación, sus instalaciones físicas, áreas críticas, recursos e información	3.4 Realizar las comunicaciones, operaciones y medidas de almacenamiento de los recursos informáticos en el tratamiento de datos personales	4.4 Prevenir el acceso no autorizado al patrimonio de la instalación, sus instalaciones físicas, áreas críticas, recursos e información	5.4 Realizar las comunicaciones, operaciones y medidas de almacenamiento de los recursos informáticos en el tratamiento de datos personales
2.1 Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas, recursos e información	2.2 Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la instalación	3.1 Prevenir que el acceso a las bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados	4.1 Prevenir que el acceso a las bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados	5.1 Prevenir que el acceso a las bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados
2.2 Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la instalación	2.3 Prevenir el acceso no autorizado al patrimonio de la instalación, sus instalaciones físicas, áreas críticas, recursos e información	3.2 Generar un esquema de protecciones para que el usuario no se vea afectado por las acciones de los usuarios no autorizados	4.2 Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la instalación	5.2 Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la instalación
2.3 Prevenir el acceso no autorizado al patrimonio de la instalación, sus instalaciones físicas, áreas críticas, recursos e información	2.4 Prevenir el acceso no autorizado al patrimonio de la instalación, sus instalaciones físicas, áreas críticas, recursos e información	3.3 Realizar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento de software y hardware	4.3 Realizar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento de software y hardware	5.3 Realizar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento de software y hardware
2.4 Prevenir el acceso no autorizado al patrimonio de la instalación, sus instalaciones físicas, áreas críticas, recursos e información	2.5 Otra medida de seguridad física (especificar)	3.4 Realizar las comunicaciones, operaciones y medidas de almacenamiento de los recursos informáticos en el tratamiento de datos personales	4.4 Prevenir el acceso no autorizado al patrimonio de la instalación, sus instalaciones físicas, áreas críticas, recursos e información	5.4 Realizar las comunicaciones, operaciones y medidas de almacenamiento de los recursos informáticos en el tratamiento de datos personales
2.5 Otra medida de seguridad física (especificar)	2.6 Prevenir el acceso no autorizado al patrimonio de la instalación, sus instalaciones físicas, áreas críticas, recursos e información	3.5 Otra medida de seguridad electrónica (especificar)	4.5 Prevenir el acceso no autorizado al patrimonio de la instalación, sus instalaciones físicas, áreas críticas, recursos e información	5.5 Otra medida de seguridad electrónica (especificar)

E1 - Política que define formalidades (normas) para la protección de datos personales	E2 - Contorno o instrumento jurídico formalizado a relación Responsable Encargado	E3 - Medidas Compensatorias	E4 - Nombre, cargo y firma de quien lo elaboró
No	No	No	Lidia Diana Angélica Jaramillo Clemente Responsable de la Unidad de Transparencia

¿Cuenta con la medida de seguridad para el tratamiento de datos personales?
No
SI
No
No
SI
No
No
No



FORMATO 4

4 ACCIONES

Acciones y Procedimientos

A4.- Nombre del Responsable

Sistema de Atención a Niños, Niñas y Adolescentes Farmacodependientes del Estado de Campeche "Vida Nueva"

No.	Acciones	C4.- Cantidad
1	Implementación de políticas internas para la gestión y tratamiento de los datos personales **	0
2	Definición de las funciones y obligaciones del personal involucrado en el tratamiento de datos personales	0
3	Elaboración de un inventario de datos personales	0
4	Elaboración de un sistema de tratamiento de datos personales	4
5	Realización de análisis de riesgos de los datos personales	0
6	Realización de análisis de brecha, comparando las medidas de seguridad existentes	0
7	Elaboración de un Plan de Trabajo para la implementación de medidas de seguridad	0
8	Elaboración de un aviso de privacidad para informar el propósito del tratamiento de los datos personales **	0
9	Monitoreo y revisión de las medidas implementadas	0
10	Diseño y aplicación de diferentes niveles de capacitación del personal	0
11	Otras acciones	0

Indicar si el responsable cuenta con lo siguiente:

Acción	Si	En caso de responder sí indicar cuántos y cuáles son:	Presentar identificación oficial que acredite la identidad del titular, o si es a través del representante debe acreditar su identidad y personalidad presentando identificación del titular y del representante, instrumento representante, domicilio, descripción clara del derecho que pretende ejercer, documentos que acrediten la representación, domicilio, descripción clara del derecho que pretende ejercer, documentos que acrediten la representación, donde señale nombre completo del titular o representante, donde señale nombre completo del titular o representante, documentos que acrediten la personalidad del titular o representante, manifestar las causas que motivan a solicitar la supresión de los datos
D4.- Procedimiento para confirmar la identidad del solicitante	SI	En caso de responder sí indicar cuántos y cuáles son:	Presentar identificación oficial que acredite la identidad del titular, o si es a través del representante debe acreditar su identidad y personalidad presentando identificación del titular y del representante, instrumento representante, domicilio, descripción clara del derecho que pretende ejercer, documentos que acrediten la representación, donde señale nombre completo del titular o representante, documentos que acrediten la personalidad del titular o representante, manifestar las causas que motivan a solicitar la supresión de los datos
E4.- Procedimiento para que un ciudadano acceda a sus datos personales	SI	En caso de responder sí indicar cuántos y cuáles son:	Presentar solicitud ante la Unidad de Transparencia, donde señale nombre completo del titular o representante, domicilio, descripción clara del derecho que pretende ejercer, documentos que acrediten la representación, donde señale nombre completo del titular o representante, documentos que acrediten la personalidad del titular o representante, manifestar las causas que motivan a solicitar la supresión de los datos
F4.- Procedimiento para que un ciudadano rectifique sus datos personales	SI	En caso de responder sí indicar cuántos y cuáles son:	Presentar solicitud ante la Unidad de Transparencia, donde señale nombre completo del titular o representante, domicilio, descripción clara del derecho que pretende ejercer, documentos que acrediten la representación, donde señale nombre completo del titular o representante, documentos que acrediten la personalidad del titular o representante, manifestar las causas que motivan a solicitar la supresión de los datos
G4.- Procedimiento para que un ciudadano cancele sus datos personales	SI	En caso de responder sí indicar cuántos y cuáles son:	Presentar solicitud ante la Unidad de Transparencia, donde señale nombre completo del titular o representante, domicilio, descripción clara del derecho que pretende ejercer, documentos que acrediten la representación, donde señale nombre completo del titular o representante, documentos que acrediten la personalidad del titular o representante, manifestar las causas que motivan a solicitar la supresión de los datos
H4.- Procedimiento para que un ciudadano se oponga al uso de sus datos personales	SI	En caso de responder sí indicar cuántos y cuáles son:	Presentar solicitud ante la Unidad de Transparencia, donde señale nombre completo del titular o representante, domicilio, descripción clara del derecho que pretende ejercer, documentos que acrediten la representación, donde señale nombre completo del titular o representante, documentos que acrediten la personalidad del titular o representante, manifestar las causas que motivan a solicitar la supresión de los datos
I4.- Procedimiento para que un ciudadano lleve a cabo la portabilidad de sus datos personales	SI	En caso de responder sí indicar cuántos y cuáles son:	El ciudadano obtiene copia de los datos personales objeto del tratamiento, el cual le permite seguir utilizándolos

J4.- Nombre, cargo y firma de quien lo elaboró.

Licda. Diana Angelica Jaramillo Clemente
 Responsable de la Unidad de Transparencia

** NOTA: Los datos proporcionados en este formato deberán coincidir respectivamente con la información proporcionada en el formato 3.