ACASyC
Abogados • Contadores • Administradores
Soluciones y Consultoría

Política de protección de datos

En cumplimiento con lo dispuesto por la **Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP),** se informa que el encargado de sus datos personales es:

Razón Social: ACASYC S.C.

Domicilio: Heráclito 309, Polanco V Sección, Miguel Hidalgo, C.P. 11560, Ciudad de México, México

Correo electrónico de contacto: Clientes@gruposyc.com
Teléfono: +52 (55) 5082 6760

Asimismo, se designa como **encargada de los mecanismos para la protección de la información** a:

Nombre: Patricia Carreto

Correo electrónico: pcarreto@gruposyc.com

Teléfono directo: +52 (55) 5082 6760

ACASYC tratará sus datos personales conforme a los principios de **licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad,** establecidos en la legislación aplicable.

FINALIDADES DEL TRATAMIENTO DE DATOS PERSONALES

Los datos personales que recabamos serán utilizados para las siguientes finalidades primarias, que son necesarias para la existencia, mantenimiento y cumplimiento de la relación jurídica con usted:

- Identificarlo y verificar su identidad.
- Proveer los servicios y productos que ha solicitado.
- Contactarlo para dar seguimiento a solicitudes, aclaraciones o quejas.
- Cumplir con obligaciones legales y contractuales.

Asimismo, utilizaremos sus datos personales para las siguientes finalidades secundarias, que no son necesarias para la relación jurídica, pero que nos permiten brindarle una mejor atención:

- Envío de información promocional, encuestas de satisfacción y boletines informativos.
- Realización de estudios de mercado y análisis estadísticos.
- Mejora de nuestros productos, servicios y experiencia de usuario.

En caso de que no desee que sus datos personales sean tratados para las finalidades secundarias, puede manifestarlo enviando un correo a: pcarreto@gruposyc.com

PROCEDIMIENTO PARA REVOCAR EL CONSENTIMIENTO

Usted puede revocar el consentimiento que, en su caso, nos haya otorgado para el tratamiento de sus datos personales. Sin embargo, es importante que tenga en cuenta que no en todos los casos podremos atender su solicitud o concluir el uso de forma inmediata, ya que es posible que por alguna obligación legal requiramos seguir tratando sus datos.

Para revocar su consentimiento, deberá enviar una solicitud al correo electrónico: pcarreto@gruposyc.com, con el asunto: **"Revocación de Consentimiento"**, e incluir la siguiente información:

1. Nombre completo del titular de los datos.
2. Medio para comunicarle la respuesta (correo electrónico o domicilio).
3. Descripción clara de los datos respecto de los cuales desea revocar el consentimiento.
4. Copia de una identificación oficial vigente.

Una vez recibida su solicitud, le daremos respuesta en un plazo máximo de **20 días hábiles**, informándole sobre la procedencia de esta. En caso de ser procedente, se hará efectiva dentro de los **15 días hábiles** siguientes a la fecha en que se le comunique la respuesta.

OBJETIVO

Esta política tiene como finalidad establecer los lineamientos para el tratamiento adecuado de los datos personales, garantizando la protección de la información, el respeto a los derechos de los titulares y el cumplimiento de los principios legales aplicables en materia de privacidad y seguridad

ALCANCE

Esta Política es aplicable a todo el personal de ACASYC, así como a sus proveedores, prestadores de servicios, contratistas, aliados comerciales, y cualquier tercero que actúe en nombre de la empresa o que mantenga una relación de negocios con ella, en la medida en que les sea aplicable. Todos los involucrados deberán observar y cumplir con los lineamientos establecidos en esta política para asegurar el correcto tratamiento y protección de los datos personales.

PROBLEMÁTICA

En el contexto actual, donde la información personal se ha convertido en un activo de alto valor, **ACASYC** reconoce los riesgos asociados al tratamiento inadecuado de los datos personales. La creciente digitalización, el intercambio constante de información y la interacción con múltiples factores externos como proveedores,

contratistas y aliados comerciales, incrementan la exposición a posibles vulneraciones de privacidad, accesos no autorizados, pérdida de datos y uso indebido de la información.

Ante este panorama, se vuelve indispensable establecer mecanismos claros y efectivos que aseguren la protección de los datos personales, tanto de clientes como de colaboradores y terceros relacionados. La falta de controles adecuados no solo representa un riesgo legal y reputacional para la empresa, sino que también puede afectar la confianza de quienes depositan su información en nuestras manos.

Por ello, **ACASYC** se compromete a implementar una política robusta que permita prevenir, detectar y responder ante cualquier incidente relacionado con la seguridad de la información y la privacidad de los datos personales, alineándose con las mejores prácticas y la normativa

Finalidades primarias del tratamiento de la información

Son aquellas que son **necesarias** para la existencia, mantenimiento y cumplimiento de la relación jurídica entre el titular de los datos y el responsable. Ejemplos:

- **Prestación de servicios contratados**: Utilizar los datos personales para brindar el servicio solicitado por el titular.
- **Facturación y gestión administrativa**: Procesar pagos, emitir comprobantes fiscales y llevar registros contables.
- **Atención al cliente**: Dar seguimiento a solicitudes, quejas o aclaraciones relacionadas con los productos o servicios.
- **Cumplimiento de obligaciones legales**: Conservar información conforme a lo requerido por leyes fiscales, laborales o de protección de datos.
- **Verificación de identidad**: Confirmar la autenticidad de los datos proporcionados para prevenir fraudes.

Finalidades secundarias del tratamiento de la información

Son aquellas que **no son necesarias** para la relación jurídica principal, pero que pueden ser útiles para mejorar servicios o realizar actividades complementarias, en este caso de forma enunciativa mas no limitativa tenemos las siguientes:

- **Envío de promociones y publicidad**: Comunicar ofertas, novedades o campañas de marketing.
- **Estudios de mercado y encuestas**: Analizar hábitos de consumo y preferencias para mejorar productos o servicios.
- **Evaluación de calidad del servicio**: Recopilar opiniones o valoraciones sobre la atención recibida.
- **Invitación a eventos o actividades**: Informar sobre conferencias, talleres, lanzamientos u otras actividades organizadas por el responsable.
- **Generación de perfiles de usuario**: Analizar el comportamiento del titular para ofrecer contenido personalizado.

SOBRE LA POLÍTICA DE PRIVACIDAD DE ACASYC

En todo tratamiento de datos personales realizado por **ACASYC**, se deberán observar los principios fundamentales de **licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad**, conforme a las disposiciones legales aplicables. Estos principios garantizan que la información personal sea tratada de manera ética, transparente y segura.

Asimismo, los datos personales deberán ser tratados con **confidencialidad**, respetando en todo momento la **expectativa razonable de privacidad** de los titulares.

1. **ACASYC** pondrá a disposición de los titulares el **Aviso de Privacidad**, conforme a los lineamientos establecidos en la legislación vigente y en concordancia con lo señalado en el apartado correspondiente de esta política.

2. La empresa contará con **medios técnicos y administrativos** que garanticen la seguridad de los datos recolectados, así como mecanismos que aseguren que el tratamiento de los datos se realice conforme a la **voluntad expresa del titular**.

3. Se designará un **responsable interno** o área encargada del tratamiento de datos personales, así como de la atención de solicitudes relacionadas con el ejercicio de los **derechos ARCO** (Acceso, Rectificación, Cancelación y Oposición).

4. La solicitud de ejercicio de **derechos ARCO** se debe realizar a través del siguiente Proceso: Enviar la solicitud al responsable del tratamiento de datos:

   Debe incluir:

   - Nombre completo del titular o representante. Documento que acredite la identidad del titular o representante (INE, Pasaporte, Cedula, etc.)
   - Domicilió o medio por el cual se le notificara.
   - Descripción detallada de los datos personales que se tengan contemplados para la solicitud.
   - Descripción del Derecho que se desea ejercer.
   - Medio de Contacto

   Estos datos una vez recabados se deben enviar al correo para recibir solicitudes ARCO.

   - Correo de contacto Patricia Carreto: pcarreto@gruposyc.com
   - Plazo de respuesta.

El responsable tiene **20 días hábiles** para responder, en caso de que proceda la solicitud se tendrá un plazo de **15 días hábiles adicionales** para poder procesar y ejecutar la acción solicitada.

- El titular podrá ejercer sus **derechos ARCO** en todo momento, siempre y cuando este ejercicio sea dentro de la vigencia del tratamiento.

5. Los lineamientos establecidos en esta política serán **vinculantes** no solo para el personal operativo, administrativo y directivo de **ACASYC**, sino también para **clientes, socios comerciales, contratistas, consultores, agentes y cualquier persona que actúe en nombre o representación de la empresa**, o que utilice medios proporcionados por esta para el tratamiento de datos personales.

6. Es responsabilidad de **ACASYC** exigir que todas las empresas con las que colabora, aquellas que le prestan cualquier tipo de servicio, con las que comercializa productos o servicios, y en general cualquier socio comercial o de negocios con el que exista intercambio de información, cumplan con los **estándares mínimos de protección de datos personales** establecidos en esta política.

7. Asimismo, **ACASYC** supervisará la implementación de políticas y procedimientos relacionados con la protección de datos personales dentro de las empresas que controla o que forman parte de su grupo corporativo, considerando sus propias condiciones, regulaciones y necesidades. Por lo tanto, esta política debe ser considerada de **estricto cumplimiento** para **ACASYC** y como **marco de referencia obligatorio** para las entidades vinculadas.

8. Esta política debe interpretarse en conjunto con otras políticas internas, procedimientos operativos y cualquier norma relacionada con **tecnologías de la información y seguridad de la información**, con el fin de garantizar un enfoque integral en la protección de los datos personales.

GENERALIDADES SOBRE LOS PRINCIPIOS DE PROTECCIÓN DE DATOS PERSONALES

El tratamiento de todos los datos personales recolectados por **ACASYC** deberá respetar, como mínimo, los siguientes principios:

1. **Licitud:** El tratamiento será considerado lícito cuando se realice conforme a la legislación aplicable, sin recurrir a medios engañosos o fraudulentos, y respetando en todo momento las expectativas razonables de privacidad de los titulares.

2. **Consentimiento:** Salvo las excepciones previstas por la ley, el tratamiento de datos personales estará sujeto al consentimiento del titular. Este consentimiento podrá ser **expreso o tácito**, según lo permita la normativa vigente. No obstante, en el caso de datos **financieros, patrimoniales o sensibles**, el consentimiento deberá ser **expreso**, salvo disposición legal en contrario. El consentimiento podrá manifestarse por cualquier medio que permita su obtención de forma clara e inequívoca.

3. **Información:** El titular de los datos personales deberá ser informado de manera clara y accesible sobre los datos que serán tratados, las finalidades específicas del tratamiento, y los medios disponibles para ejercer sus derechos. Además, **ACASYC** se compromete a comunicar oportunamente cualquier cambio en los fines, medios o condiciones bajo las cuales se realiza el tratamiento de los datos personales.

4. **Calidad y Proporcionalidad:** Los datos personales recolectados por **ACASYC** deberán ser **exactos, completos, pertinentes, correctos y actualizados**, conforme a lo necesario para cumplir con las finalidades para las cuales fueron obtenidos. Asimismo, únicamente se tratarán aquellos datos que sean **necesarios, adecuados y relevantes** en relación con dichas finalidades, evitando la recopilación excesiva o innecesaria de información.

5. **Finalidad:** El tratamiento de los datos personales por parte de **ACASYC** deberá limitarse exclusivamente a las finalidades establecidas en el **Aviso de Privacidad**, para las cuales el titular haya otorgado su consentimiento. No se permitirá el uso de los datos para fines distintos sin una nueva autorización expresa del titular.

6. **Confidencialidad:** En ninguna circunstancia los datos personales podrán ser divulgados, compartidos o publicados a terceros sin el consentimiento previo del titular. **ACASYC** aplicará en todo momento medidas técnicas, administrativas y físicas que garanticen la seguridad y confidencialidad de la información.

7. **Responsabilidad: ACASYC**, como responsable del tratamiento, está obligada a velar por el cumplimiento de esta política y responder por el uso adecuado de los datos personales que se encuentren bajo su custodia o posesión, incluyendo aquellos tratados por terceros en su nombre.

SOBRE EL TRATAMIENTO DE LOS DATOS PERSONALES RECABADOS POR ACASYC

OBTENCION DE LOS DATOS PERSONALES

1. **ACASYC** establecerá y documentará los procedimientos necesarios para la **recolección, uso, almacenamiento y tratamiento de datos personales** de todas las personas con las que mantiene relación profesional o comercial, incluyendo **clientes, empleados, proveedores, socios estratégicos y terceros vinculados**. Estos procedimientos estarán alineados con los principios legales aplicables y se implementarán con el objetivo de garantizar la protección, confidencialidad y uso responsable de la información personal.

2. **Datos Personales Recabados con la Finalidad del Tratamiento**,

   Se podrá recabar y tratar los siguientes **datos personales** del titular, con el fin de cumplir con las obligaciones derivadas de la relación jurídica que se establezca, así como para fines administrativos, comerciales, de contacto y cumplimiento normativo:

   Los datos personales que podrá recabar incluyen, de manera enunciativa mas no limitativa:

- **Datos de Identificación**: Nombre completo, fecha de nacimiento, CURP, RFC, firma autógrafa o electrónica.
- **Datos de contacto**: Domicilio, número telefónico, correo electrónico.
- **Datos laborales:** Puesto, área o departamento, historial profesional.
- **Datos financieros**: información bancaria, historial crediticio, ingresos.
- **Datos electrónicos**: dirección IP, ubicación geográfica, hábitos de navegación, tipo de dispositivo.

En caso de que se recaben **datos personales sensibles**, como estado de salud, datos biométricos o creencias religiosas, se solicitará el **consentimiento expreso** del titular, conforme a lo establecido en la legislación aplicable, (**Artículo 15 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO))**

El tratamiento de los datos personales se realizará conforme a los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad establecidos en la LFPDPPP.

3. **La recolección de datos personales por parte de ACASYC podrá realizarse a través de diversos medios**, incluyendo la atención presencial, comunicaciones por correo electrónico, llamadas telefónicas, formularios en línea, sitios web institucionales, así como fuentes de acceso público, entre otros canales legítimos. En todos los casos, se garantizará que el tratamiento de la información se realice conforme a los principios de legalidad, transparencia y respeto a la privacidad del titular.

4. **ACASYC podrá obtener datos personales de manera indirecta a través de terceros**, siempre y cuando se verifique previamente que la persona o entidad que realiza la transferencia cuenta con la **autorización legal o el consentimiento válido del titular** para hacerlo. Esta práctica se llevará a cabo conforme a la normativa aplicable y bajo estrictos criterios de legalidad, confidencialidad y responsabilidad en el manejo de la información.

5. En los casos en que se requiera obtener datos personales de **menores de edad**, personas con **incapacidad legal declarada** o en **estado de interdicción**, **ACASYC** deberá solicitar el **consentimiento expreso** de los **padres, tutores o representantes legales** del titular. Esta autorización deberá ser otorgada conforme a lo establecido en el **Aviso de Privacidad**, garantizando que el tratamiento de la información se realice de manera legal, ética y respetuosa de los derechos de los titulares en situación de vulnerabilidad.

RESGUARDO DE LOS DATOS PERSONALES

1. El resguardo de los datos personales en **ACASYC** se realizará mediante sistemas de almacenamiento **físicos y/o electrónicos**, implementando medidas de seguridad **razonables, proporcionales y adecuadas** para proteger la integridad, confidencialidad y disponibilidad de la información. El acceso a estas bases de datos estará **restringido exclusivamente al personal autorizado**, responsable del tratamiento de los datos personales.

2. Además, el encargado del tratamiento deberá mantener un **inventario actualizado** que identifique los datos personales bajo su custodia, así como los sistemas, aplicaciones o plataformas utilizadas para su procesamiento, incluyendo aquellas que operen bajo esquemas de **infraestructura tecnológica externa**, como el **cómputo en la nube**, siempre garantizando el cumplimiento de las disposiciones legales aplicables y los estándares de seguridad de la información.

3. **ACASYC** deberá implementar mecanismos de **control de acceso** que limiten la manipulación de datos personales únicamente al personal autorizado, según su rol y nivel de responsabilidad. Además, se establecerán sistemas de **registro y trazabilidad** que permitan auditar las acciones realizadas sobre la información, como accesos, modificaciones, transferencias o eliminaciones, con el fin de detectar posibles incidentes de seguridad, garantizar la rendición de cuentas y facilitar la respuesta ante cualquier eventualidad.

BLOQUEO DE LOS DATOS PERSONALES

1. En ACASYC, el bloqueo de datos personales se aplicará cuando, habiendo cumplido la finalidad para la cual fueron recabados, no sea posible su eliminación inmediata por razones legales, contractuales o administrativas. Durante el periodo de bloqueo, los datos permanecerán restringidos y sin ser objeto de tratamiento, salvo para fines de conservación o cumplimiento de obligaciones legales.

2. Este proceso garantiza que la información no sea utilizada indebidamente mientras se mantiene en resguardo, y se aplicarán medidas de seguridad que aseguren su **integridad, confidencialidad y no acceso no autorizado**. Una vez concluido el plazo legal o administrativo correspondiente, los datos serán eliminados de forma segura.

3. **ACASYC** deberá realizar **revisiones periódicas** del estado de los datos personales que se encuentren en condición de bloqueo, con el fin de verificar si persisten las razones legales, contractuales o administrativas que impiden su eliminación. Esta práctica permitirá mantener actualizada la base de datos, evitar el almacenamiento innecesario de información y asegurar que los datos bloqueados sean eliminados de forma segura una vez que haya cesado la causa que justificaba su conservación.

SUPRESION DE LOS DATOS PERSONALES

1. Una vez cumplida la finalidad para la cual fueron recabados los datos personales, o transcurrido el plazo legal o contractual correspondiente, el titular podrá solicitar su **cancelación**, lo que conlleva la **supresión definitiva** de dicha información de las bases de datos de **ACASYC**.

2. La supresión implica la **eliminación, destrucción o borrado seguro** de los datos personales, conforme a los protocolos establecidos por la empresa y aplicando las **medidas de seguridad necesarias** para evitar cualquier acceso, uso o recuperación no autorizada. Este proceso se realizará de manera responsable, garantizando el respeto a los derechos del titular y el cumplimiento de las disposiciones legales aplicables.

3. El responsable del tratamiento de datos personales en **ACASYC** deberá implementar **métodos y técnicas eficaces** para garantizar la **eliminación definitiva** de la información personal una vez que haya concluido su ciclo de vida o se haya autorizado su cancelación. Estos procedimientos deberán asegurar que la **probabilidad de recuperación o reutilización de los datos sea mínima o nula**, aplicando estándares de **borrado seguro**, tanto en medios físicos como digitales.

4. Las técnicas utilizadas deberán estar alineadas con las mejores prácticas en seguridad de la información, incluyendo la destrucción física de documentos, el borrado criptográfico de archivos electrónicos, y la eliminación segura en entornos de almacenamiento en la nube, cuando corresponda.

TRANSFERENCIA Y REMISION

ACASYC podrá realizar la **transferencia de datos personales a terceros**, siempre que cuente con el **consentimiento previo y válido del titular**, y que dicha transferencia esté permitida por la legislación aplicable. Antes de llevar a cabo cualquier transferencia, se verificará que el tercero receptor ofrezca **niveles de protección de datos personales equivalentes o superiores** a los establecidos en esta política, y que cumpla con los **marcos normativos vigentes en materia de privacidad y protección de datos**.

Este proceso tiene como objetivo asegurar que la información personal continúe siendo tratada con los más altos estándares de seguridad y confidencialidad, incluso fuera del entorno directo de **ACASY.** Se podrá celebrar acuerdos de transferencia de datos donde se deberá de contemplar como mínimo lo siguiente:

1. Los datos específicos para transferir. Política controlada por el Área de Control Interno
2. La naturaleza de los datos transferidos en relación con la necesidad de consentimiento para la transferencia.
3. Las medidas de protección y de seguridad.
4. Requerir al tercero que se comprometa a que sus medidas de protección. y de seguridad estén de acuerdo con la presente Política.
5. Estipular mecanismos de consulta para monitorear la transferencia de datos y la seguridad de estos.

VULNERACION

En ACASYC, se considera que existe una **vulneración a los datos personales** cuando se produce cualquier incidente que comprometa la confidencialidad, integridad o disponibilidad de la información personal. Esto incluye, pero no se limita a:

a) Pérdida, destrucción o daño de datos por causas accidentales o intencionales.
b) Robo, extravío o copia no autorizada de información contenida en medios físicos o digitales.
c) Acceso, uso o tratamiento indebido por parte de personas no autorizadas.
d) Alteración, modificación o manipulación no consentida de los datos.
e) Divulgación, revelación o exposición no autorizada de información personal a terceros.

f) También se considerará vulneración de datos personales cualquier **incidente de seguridad** que afecte el tratamiento de dicha información, incluyendo accesos no autorizados, alteraciones indebidas o cualquier evento que comprometa su protección.

g) De forma preventiva, el responsable y/o encargado del tratamiento de datos personales deberá implementar **controles de seguridad** y **mecanismos de respuesta** que permitan actuar eficazmente ante posibles incidentes relacionados con la protección de la información en la que se contempla lo siguiente

h) **La mejora continua** consiste en documentar detalladamente las acciones realizadas ante un incidente de seguridad, así como en comunicar a las partes interesadas el estado actual de los activos de información. Esta documentación debe integrarse en una bitácora o archivo de referencia, que sirva como base de conocimiento para fortalecer los procesos internos y capacitar a nuevos integrantes del equipo de respuesta a incidentes.

i) **La identificación** consiste en detectar y analizar las alertas de seguridad que puedan estar relacionadas con el tratamiento de datos personales. El objetivo es determinar si dichas alertas deben clasificarse como incidentes de seguridad que representen una posible vulneración. ACASYC deberá documentar de forma sistemática todas las alertas relevantes, especialmente aquellas que puedan derivar en riesgos para la integridad, confidencialidad o disponibilidad de los datos personales. Esta documentación servirá como base para la toma de decisiones, la mejora de los controles internos y la activación de protocolos de respuesta.

j) La **contención** tiene como objetivo **limitar el alcance y reducir el impacto** de un incidente de seguridad una vez identificado. Para ello, ACASYC deberá ordenar el **aislamiento inmediato de los activos comprometidos**, así como la **generación de respaldos de seguridad** que permitan preservar la información y facilitar su recuperación

k) La **mitigación** consiste en aplicar medidas correctivas para **reducir el riesgo de recurrencia** del incidente de seguridad. ACASYC deberá **recolectar evidencia técnica** para realizar un análisis forense del evento, identificar su causa raíz y **reforzar los controles de seguridad** que protegen los datos personales.

l) La **recuperación** consiste en dar seguimiento a las medidas aplicadas durante la mitigación, asegurando que los **activos afectados** sean reintegrados de forma segura a los sistemas de tratamiento. ACASYC deberá **monitorear el funcionamiento** de los sistemas y validar la efectividad de las nuevas medidas adoptadas. Una vez erradicado el incidente, se deberá **emitir un reporte final** que documente el proceso y los resultados obtenidos.

SOBRE EL SEGUIMIENTO POR PARTE DEL ENCARGADO DE PROTECCION DE DATOS

El responsable del tratamiento deberá informar al titular sobre cualquier vulneración de seguridad que afecte sus datos personales en cualquier fase del proceso. Asimismo, deberá elaborar un informe detallado que incluya, al menos, los siguientes elementos:

a) Fecha y hora en que se **detectó la vulneración**.

b) Fecha y hora en que **inició la investigación** del incidente.

c) **Tipo y naturaleza** del incidente ocurrido.

d) **Datos personales comprometidos** durante el evento.

e) **Descripción detallada** de las circunstancias que rodearon la vulneración.

f) **Sistemas de tratamiento** que fueron afectados.

g) **Medidas correctivas inmediatas** que se implementaron.

h) **Posibles consecuencias** derivadas del incidente de seguridad.

i) **Recomendaciones** para prevenir futuras vulneraciones.

j) **Documentación complementaria** que respalde el reporte.

k) **Medios de contacto** para obtener información adicional sobre el caso.

En caso de que la vulneración de datos personales implique hechos con posible carácter delictivo, el responsable deberá remitir el informe correspondiente a las autoridades competentes.

Asimismo, ACASYC tendrá la obligación de notificar a los titulares sobre cualquier incidente relacionado con el tratamiento de sus datos personales, en cualquiera de los siguientes tres momentos:

1. Tan pronto como sea posible, una vez detectada la vulneración.
2. Cuando se disponga de información precisa sobre el incidente.
3. Al momento en que los activos comprometidos ya no estén expuestos o en riesgo.

MEDIDAS DE SEGURIDAD ORGANIZATIVA Y DE COLABORADORES

Además de las responsabilidades previamente mencionadas, el encargado del tratamiento de datos personales será responsable de elaborar un inventario actualizado de los datos personales bajo resguardo, utilizando herramientas tecnológicas que faciliten su clasificación y control.

Asimismo, bajo la supervisión del área legal y de cumplimiento, deberá desarrollar el documento de seguridad, el cual incluirá las medidas, controles y acciones preventivas aplicables al tratamiento de datos personales. Estas medidas deberán estar organizadas en tres categorías:

Administrativas

(a) **Capacitación continua al personal:** Formación periódica sobre el manejo adecuado de datos personales, buenas prácticas de seguridad y cumplimiento normativo.
(b) **Control de acceso basado en funciones:** Definición clara de roles y responsabilidades, limitando el acceso a los datos personales únicamente al personal autorizado según sus funciones.
(c) Políticas internas de confidencialidad: Establecimiento de lineamientos que regulen el uso, divulgación y protección de la información, incluyendo acuerdos de confidencialidad firmados por el personal.
(d) Evaluaciones periódicas de cumplimiento: Revisión regular de los procesos internos para verificar el cumplimiento de la normativa en materia de protección de datos personales.
(e) Gestión documental y trazabilidad: Registro y control de todos los procesos relacionados con el tratamiento de datos, permitiendo identificar quién accedió, cuándo y con qué propósito.

Físicas

Las medidas físicas tienen como objetivo **proteger el entorno físico** donde se resguardan y procesan los datos personales, evitando accesos no autorizados, daños o pérdidas. Entre las principales acciones que ACASYC implementa se encuentran:

(a) **Restringir el acceso físico** a las instalaciones, áreas sensibles, equipos y documentos, mediante controles como llaves, tarjetas electrónicas o registros de ingreso.
(b) **Evitar daños o interferencias** en zonas críticas mediante protocolos de seguridad y supervisión constante.
(c) **Protege dispositivos móviles, portátiles y soportes físicos o electrónicos** que puedan salir de la oficina, asegurando su resguardo y transporte seguro.
(d) **Realiza mantenimiento preventivo y correctivo** a los equipos que almacenan datos personales, garantizando su disponibilidad, integridad y funcionamiento óptimo.
(e) **Instalación sistemas de videovigilancia (CCTV)** en puntos estratégicos de la oficina, con fines de monitoreo, control de accesos y prevención de incidentes.

Técnicas

Las medidas técnicas están orientadas a proteger los sistemas informáticos, redes y plataformas digitales utilizadas en el tratamiento de datos personales. Su propósito es prevenir accesos no autorizados, alteraciones, pérdidas o divulgaciones indebidas, mediante herramientas y configuraciones que refuercen la seguridad digital.

(a) **Uso de contraseñas robustas y autenticación multifactor (MFA)**
Para restringir el acceso a sistemas y plataformas que contienen datos personales.
(b) **Cifrado de información**
Aplicación de técnicas de encriptación en el almacenamiento y transmisión de datos para evitar su lectura por terceros no autorizados.
(c) **Actualización constante de software y sistemas**
Instalación regular de parches de seguridad y versiones actualizadas para prevenir vulnerabilidades.

(d) **Monitoreo y registro de actividades**
Implementación de sistemas de auditoría que permitan rastrear accesos, modificaciones y eventos relevantes en los sistemas.

(e) Antivirus y herramientas de detección de amenazas
Uso de soluciones tecnológicas que identifiquen y bloqueen malware, intrusiones o comportamientos sospechosos.

PLAZOS DE CONSERVACIÓN DE LOS DATOS PERSONALES

Los datos personales que recabamos serán conservados únicamente durante el tiempo que sea necesario para cumplir con las finalidades para las cuales fueron recabados, y conforme a lo establecido en la **Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP)** y demás normativas aplicables.

Una vez cumplida la finalidad del tratamiento, y siempre que no exista una obligación legal o contractual que requiera su conservación, los datos serán eliminados o anonimizados de forma segura.

En casos específicos, los plazos de conservación podrán extenderse cuando:

- Exista una obligación legal de conservar los datos (por ejemplo, fiscales o contables).
- Sea necesario para el ejercicio o defensa de un derecho en un procedimiento judicial.
- El titular haya otorgado su consentimiento para un tratamiento posterior compatible con las finalidades originales.

CUMPLIMIENTO DEL DERECHO INTERNACIONAL EN MATERIA DE PRIVACIDAD

Acasyc se compromete a respetar los principios del **derecho internacional en materia de protección de datos personales**, conforme a los tratados y normas suscritos por los Estados Unidos Mexicanos, incluyendo:

- El **Convenio 108 del Consejo de Europa** y su **Protocolo Adicional**, ratificados por México y publicados en el Diario Oficial de la Federación, los cuales establecen estándares internacionales para el tratamiento automatizado de datos personales y regulan los flujos transfronterizos de datos. [gob.mx]
- El **Artículo 16, segundo párrafo, de la Constitución Política de los Estados Unidos Mexicanos**, que reconoce el derecho a la protección de datos personales.
- La **Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO)** y la **Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP)**, que regulan el tratamiento de datos por parte de entidades públicas y privadas, respectivamente.
- Los principios establecidos en instrumentos internacionales como la **Declaración Universal de los Derechos Humanos** (art. 12) y el **Pacto Internacional de Derechos Civiles y Políticos** (art. 17), ambos ratificados por México.

En caso de transferencias internacionales de datos personales, garantizamos que se aplicarán mecanismos jurídicos adecuados, como **cláusulas contractuales tipo**, **normas corporativas vinculantes**, o que el país receptor cuente con un nivel de protección equivalente conforme a los estándares internacionales y nacionales aplicables.

Asimismo, nos comprometemos a cooperar con las autoridades de protección de datos nacionales e internacionales, y a garantizar el ejercicio de los derechos ARCO (Acceso, Rectificación, Cancelación y Oposición) por parte de los titulares de los datos.

MECANISMOS DE ACTUALIZACIÓN DE LA POLÍTICA DE PRIVACIDAD

Esta política de privacidad podrá modificarse o actualizarse en cualquier momento, según las disposiciones legales aplicables y conforme a las necesidades de nuestros servicios, prácticas internas o nuevas disposiciones normativas.

Cualquier cambio sustancial será comunicado a través de los siguientes medios:

- Publicación visible en nuestro sitio web:
- Correo electrónico dirigido a los titulares de los datos, cuando sea posible.
- Avisos físicos en nuestras instalaciones, en caso de atención presencial.

Se recomienda al titular revisar periódicamente esta política para estar informado sobre cómo protegemos sus datos personales. La fecha de la última actualización se indicará al final del documento.

Última actualización: 02 de enero de 2025

GLOSARIO DE TERMINOS Y PALABRAS CLAVE PARA EFECTOS DE LA PRESENTE POLITICA.

ALERTA DE SEGURIDAD: Notificaciones que se envían al usuario para informarle sobre posibles riesgos o actividades sospechosas relacionadas con la seguridad de su cuenta, sus datos personales o el uso de los servicios. Estas alertas pueden incluir intentos de acceso no autorizados, cambios en la configuración de seguridad, vulnerabilidades detectadas, o cualquier evento que pueda comprometer la integridad, confidencialidad o disponibilidad de la información.

Vulneración: Se refiere a cualquier incidente que comprometa la seguridad, confidencialidad, integridad o disponibilidad de los datos personales. Esto puede incluir accesos no autorizados, pérdida, destrucción, alteración o divulgación indebida de información personal, ya sea de forma accidental o intencional.

Tratamiento: Conjunto de operaciones realizadas sobre datos personales, ya sea por medios automatizados o no. Incluye la recopilación, registro, organización, conservación, modificación, extracción, consulta, uso, comunicación, difusión, y cualquier otra forma de manejo de dichos datos.

Transferencia: Acción mediante la cual los datos personales se envían o comparten con un tercero, dentro del mismo país o a nivel internacional. Esta transferencia puede realizarse con fines operativos, legales, comerciales o de seguridad, siempre bajo condiciones que garanticen la protección adecuada de la información.

Supresión: Eliminar o borrar datos personales cuando ya no son necesarios para los fines para los que se recopilaron, o cuando el titular de los datos solicita su eliminación según sus derechos. La supresión puede implicar la destrucción física o la eliminación lógica de los datos en los sistemas.

Robo: Acceso, apropiación o extracción no autorizada de datos personales por parte de terceros, generalmente con fines maliciosos. El robo de datos representa una grave vulneración a la privacidad y puede derivar en fraudes, suplantación de identidad u otros delitos.

Responsable: Persona física o moral que decide sobre el tratamiento de los datos personales. Es quien determina los fines y medios del tratamiento, y tiene la obligación de garantizar la protección, confidencialidad y seguridad de los datos conforme a la legislación aplicable.

Remisión: Proceso por el cual los datos personales se envían o comparten con un tercero que actúa en nombre del responsable del tratamiento para prestar un servicio. A diferencia de la transferencia, en la remisión el tercero no decide sobre el uso de los datos, sino que los trata conforme a las instrucciones del responsable.

Pérdida: Situación en la que los datos personales dejan de estar disponibles o accesibles de forma permanente o temporal, ya sea por causas accidentales, técnicas o por negligencia. La pérdida puede afectar la continuidad del servicio y comprometer la privacidad del titular.

Titular: Persona física a quien corresponden los datos personales. Es quien tiene el derecho de conocer, acceder, rectificar, cancelar u oponerse al tratamiento de sus datos, conforme a la legislación aplicable en materia de protección de datos.

Obtención de información indirecta: Proceso mediante el cual se recopilan datos personales sin que el titular los proporcione directamente, sino a través de fuentes externas o mediante el uso de tecnologías como cookies, sensores, registros de actividad, terceros autorizados, o integraciones con otras plataformas. Esta información puede incluir hábitos de navegación, ubicación, preferencias de uso, entre otros, y debe ser obtenida conforme a los principios de licitud, consentimiento y transparencia establecidos por la legislación aplicable.

Obtención de información de forma directa: Proceso por el cual el titular proporciona los datos personales, generalmente mediante formularios, registros, encuestas, contratos, aplicaciones o cualquier otro medio en el que el usuario ingresa consciente y explícitamente su información. Esta forma de obtención garantiza que el titular conoce qué datos está entregando y con qué propósito serán utilizados.

Obtención de información de forma personal: Recopilación de datos personales realizada directamente por el responsable o su personal autorizado, mediante interacción presencial con el titular. Esto puede ocurrir en oficinas, sucursales, eventos, entrevistas, o cualquier otro punto de contacto físico, donde el titular proporciona su información verbalmente, por escrito o a través de dispositivos habilitados para tal fin.

Medidas de seguridad administrativas: Conjunto de políticas, procedimientos y controles internos establecidos por el responsable del tratamiento para garantizar la protección de los datos personales. Estas medidas incluyen la capacitación del personal, la asignación de responsabilidades, la gestión de accesos, la supervisión de procesos, la evaluación de riesgos, y la implementación de protocolos para la atención de incidentes de seguridad. Su objetivo es prevenir el uso indebido, acceso no autorizado o pérdida de información.

Medidas de seguridad técnicas: Controles y mecanismos tecnológicos implementados para proteger los datos personales contra accesos no autorizados, alteraciones, pérdidas o divulgaciones indebidas. Estas medidas incluyen el uso de cifrado, firewalls, antivirus, autenticación multifactorial, monitoreo de sistemas, y actualizaciones periódicas de software, entre otros.

Medidas de seguridad físicas: Acciones y recursos destinados a proteger los espacios donde se almacenan o procesan datos personales, evitando accesos no autorizados o daños materiales. Incluyen el control de acceso a instalaciones, vigilancia, cerraduras, almacenamiento seguro de documentos físicos, y protección de equipos informáticos.

Incidente de seguridad: **Evento** que afecta o pone en riesgo la confidencialidad, integridad o disponibilidad de los datos personales. Puede incluir accesos no autorizados, pérdida, alteración, divulgación indebida, robo o cualquier otra situación que comprometa la seguridad de la información.

Extravió: Situación en la que los datos personales se pierden o se desconoce su ubicación, ya sea por error humano, fallas técnicas o negligencia. El extravío puede representar un riesgo para la privacidad del titular si los datos quedan expuestos o accesibles a terceros no autorizados.

Encargado: Persona física o moral que trata datos personales por cuenta del responsable. El encargado actúa conforme a las instrucciones del responsable y está obligado a cumplir con las medidas de seguridad y confidencialidad establecidas por la legislación aplicable.

Documento de seguridad: Instrumento que describe las políticas, procedimientos y medidas implementadas para proteger los datos personales. Incluye aspectos como el control de accesos, gestión de riesgos, protocolos de respuesta ante incidentes, y responsabilidades del personal involucrado en el tratamiento de datos.

Divulgación no autorizada: Acción por la que los datos personales se comparten, publican o comunican a terceros sin el consentimiento del titular o sin cumplir con los requisitos legales. Esta divulgación puede ser accidental o intencional y representa una vulneración a la privacidad.

Destrucción: Proceso por el que los datos personales se eliminan de forma definitiva, ya sea en formato físico o digital, asegurando que no puedan recuperarse ni usarse después. La destrucción debe realizarse conforme a procedimientos seguros y documentados.

Derecho de oposición: Facultad que tiene el titular de los datos personales para solicitar que no se lleve a cabo el tratamiento de sus datos en determinados casos, especialmente cuando dicho tratamiento no sea necesario para cumplir una obligación legal o contractual. Este derecho permite al titular proteger sus intereses legítimos.

Derecho de cancelación: Facultad del titular para solicitar la eliminación de sus datos personales cuando considere que no están siendo tratados conforme a los principios, deberes y obligaciones establecidas por la ley. Este derecho permite que los datos sean suprimidos de las bases de datos del responsable, salvo que exista una obligación legal para conservarlos.

Derecho de rectificación: Derecho que tiene el titular para solicitar la corrección de sus datos personales cuando estos sean inexactos, incompletos o estén desactualizados. El responsable debe realizar la rectificación en un plazo razonable y notificar al titular sobre el cambio.

Derecho de acceso: Facultad del titular para conocer si sus datos personales están siendo tratados, qué datos se poseen, con qué finalidad, el origen de estos y las comunicaciones realizadas o previstas. Este derecho permite al titular tener control sobre el uso de su información.

Derechos ARCO: Conjunto de derechos que protegen los datos personales de los individuos: **Acceso, Rectificación, Cancelación y Oposición**. Estos derechos permiten al titular ejercer control sobre su información personal y exigir su correcto tratamiento conforme a la legislación de protección de datos

Datos sensibles: Información personal que afecta los aspectos más íntimos del titular, cuyo uso indebido puede dar lugar a discriminación o poner en riesgo su integridad. Incluyen datos sobre origen étnico o racial, estado de salud, creencias religiosas, filosóficas o morales, afiliación sindical, opiniones políticas, orientación sexual, y datos biométricos.

Datos personales: Cualquier información que identifica o hace identificable a una persona física. Esto incluye nombre, dirección, correo electrónico, número telefónico, identificaciones oficiales, datos financieros, entre otros. Su tratamiento debe realizarse conforme a los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad.

Daño: Consecuencia negativa del titular por el tratamiento indebido de sus datos personales. Puede ser material, moral, reputacional o económico, y puede derivarse de incidentes como divulgación no autorizada, robo, pérdida o alteración de la información.

Copia no autorizada: Reproducción o duplicación de datos personales sin el consentimiento del titular ni la autorización del responsable. Esta acción puede representar una vulneración a la privacidad y a la seguridad de la información.

Consentimiento tácito: Autorización que se presume otorgada por el titular cuando, habiendo sido informado sobre el tratamiento de sus datos personales, no manifiesta oposición en un plazo razonable. Este tipo de consentimiento solo es válido cuando la ley lo permite y siempre que se haya proporcionado información clara y suficiente.

Consentimiento expreso: Autorización otorgada de manera clara y directa por el titular para el tratamiento de sus datos personales. Puede ser verbal, escrita o mediante medios electrónicos, y debe ser previa al tratamiento, especialmente cuando se trata de datos sensibles o transferencias internacionales.

Consentimiento: Manifestación de la voluntad del titular mediante la cual autoriza el tratamiento de sus datos personales. Puede ser tácito o expreso, y debe otorgarse de forma libre, específica, informada e inequívoca, conforme a lo establecido por la legislación aplicable

Bloqueo: Medida de seguridad que consiste en restringir el acceso o tratamiento de los datos personales, conservándolos solo para cumplir obligaciones legales o contractuales. El bloqueo se aplica cuando el titular ejerce derechos como cancelación u oposición, o durante la revisión de un incidente de seguridad.

Aviso de privacidad: Documento físico, electrónico o en cualquier otro formato que informa al titular sobre la existencia del tratamiento de sus datos personales, las finalidades de este, la identidad del responsable, los derechos que le asisten y los mecanismos para ejercerlos. Es obligatorio y debe ser claro, accesible y actualizado.

Brecha de seguridad: Evento que compromete la protección de los datos personales, como accesos no autorizados, pérdida, destrucción, alteración o divulgación indebida. Las brechas de seguridad deben ser gestionadas conforme a protocolos establecidos y, en ciertos casos, notificadas a las autoridades y a los titulares afectados.

_____

Florentina Soberon Peñaloza

_____

Patricia Carreto

ANEXOS

FORMATO DE IDENTIFICACIÓN DE INCIDENTES EN ACASyC

INFORMACIÓN GENERAL

Información del personal que detecta el incidente

Nombre:					
Dirección:					
Teléfono:		Teléfono alterno:		Celular:	
Ext/Fax:		Correo electrónico:			

Información del personal que detecta el incidente				
Fecha:		Hora:		
Localización dónde se detectó el incidente:				
Tipo de sistema de tratamiento:	( )	Físico	( )	Electrónico
Nombre del responsable del tratamiento:				
¿Se encuentran involucrados datos personales en el incidente?:	( )	Sí	( )	No

Tipos de datos personales involucrados:	
Descripción de lo sucedido:	

Evaluación (para ser llenado por el equipo de gestión de incidentes				
Una vez analizada la información, se determina que se trata de un incidente de seguridad:	( )	Sí	( )	No

Justificación:
Menciona si existe algún posible impacto legal o contractual por el incidente:

RESUMEN DEL INCIDENTE

RESUMEN EJECUTIVO DEL INCIDENTE

RESUMEN TÉCNICO DEL INCIDENTE						
Tipo de incidente	( )	Denegación de servicio	( )	Uso no autorizado	( )	Espionaje
	( )	Código malicioso	( )	Acceso no autorizado	( )	Robo, pérdida o extravío
	( )	ingeniería social	( )	Otro:		

Sitio/Área/Departamento dónde se presentó el incidente:	
Nombre del contacto en el sitio dónde se presentó el incidente:	

Dirección:					
Teléfono:		Teléfono alterno:		Celular:	
Ext/Fax:		Correo electrónico:			
¿Cómo fue detectado el incidente?					
Información adicional					
Firma					
Nombre y firma del personal que detecta el incidente			Nombre y firma del personal representante del Equipo de Gestión de Incidentes		

- **FORMATO DE INVESTIGACIÓN DEL INCIDENTE EN ACASyC**

DATOS PARA INVESTIGACIÓN

Ubicación de los sistemas de tratamiento afectados

Sistema afectado:		Sitio:	

Tiempos

Fecha y hora en que se detectó el incidente		Fecha y hora en que los especialistas en incidentes llegaron al sitio	
Fecha:		Fecha:	
Hora:		Hora:	

Descripción

Sistema de tratamiento afectado:				
¿El sistema de tratamiento afectado es físico o electrónico?	( )	Físico	( )	Electrónico

SISTEMAS DE TRATAMIENTO FÍSICO

Sistema de tratamiento:	
Describa los controles de seguridad físicos que identifique de la inspección ocular:	
Personas que tienen acceso al sistema de tratamiento:	

SISTEMAS DE TRATAMIENTO ELECTRÓNICO

Sistema de tratamiento:				
Describa los controles de seguridad electrónicos que identifique de la inspección ocular:				
¿El sistema afectado está conectado a una red?	( )	Si	( )	No

Dirección de red del sistema:		Dirección MAC:	

¿El sistema afectado está conectado a un punto de acceso a Internet?	( )	Si	( )	No
Número de teléfono:				

¿Se contrataron los servicios de personal externo para apoyar o realizar la gestión del incidente?
Si/No Describir las acciones realizadas por el personal externo para la gestión o apoyo del incidente.

- **FORMATO DE INVESTIGACIÓN DEL INCIDENTE**

ACCIONES DE CONTENCIÓN

1. Aislamiento de los sistemas de tratamiento afectados:

¿El Comité de Respuesta a Incidentes aprobó el aislamiento/bloqueo/resguardo?	( )	Si	( )	No

Acción aprobada	( )	Aislamiento	( )	Bloqueo	( )	Resguardo	( )	Reubicación

Si				No
Hora:		Fecha:		Describir la razón de la negativa

2. Respaldo de los sistemas afectados:

¿Se cuenta con respaldo del sistema de tratamiento afectado?	( )	Si	( )	No
Si no se cuenta con respaldos, ¿es necesario respaldar?	( )	Si	( )	No
Si se realizó un respaldo ¿fue exitoso para todos los sistemas?	( )	Si	( )	No

Acciones realizadas para hacer el respaldo:			
Nombres de las personas que realizaron el respaldo:			
Fecha de inicio del respaldo:		Fecha de término del respaldo:	
Hora de inicio del respaldo:		Hora del término del respaldo:	

Mecanismo empleado para el respaldo
Físicos

( )	Copias fotostáticas	( )	Sitio alterno	( )	Otro:

Electrónicos

( )	Cintas	( )	CD/DVD/USB	( )	Digitalización
( )	Disco duro	( )	Nube	( )	Otro:

¿El mecanismo de respaldo fue sellado?	( )	Si	( )	No

Fecha del sello:		Hora del sello:	
Nombre de la persona a quién fue entregado el respaldo o es responsable de su resguardo:			
Sitio dónde se almacenó el respaldo:			

¿Se realizaron pruebas al respaldo?	( )	Si	( )	No

Mecanismos utilizados para las pruebas	

Nombre y firma de quién realiza el respaldo	Nombre y firma de quién recibe y valida el respaldo

- FORMATO DE MITIGACIÓN DEL INCIDENTE

DESCRIPCIÓN DE LAS ACCIONES DE MITIGACIÓN

1. Personal involucrado
Nombre de las personas que realizaron el análisis del sistema de tratamiento afectado:

Iniciales	Nombre completo	Puesto

2. Descripción de las vulnerabilidades detectadas:

¿Fueron identificadas vulnerabilidades?	( )	Si	( )	No

Tipo de activo	Vulnerabilidad	Descripción	Impacto

Acciones realizadas para erradicar las vulnerabilidades detectadas

3. Validación:

¿Cuál fue el procedimiento de validación usado para asegurar que el problema fue erradicado?

4. Cierre:

Fecha y hora del cierre del incidente:	
Nombre y firma de quién realiza la erradicación	Nombre y firma de quién validó la erradicación

- **FORMATO DE MITIGACIÓN DEL INCIDENTE**

PROCESAMIENTO DE INDICIOS O EVIDENCIA

1. Identificación de los indicios o evidencia:

Número de indicio o evidencia	Descripción de indicio o evidencia	Estado en que encontraba
1	Si es un dispositivo físico, incluir modelo y número de serie	
2		
3		

2. Fijación de los indicios o evidencias:

Fotográfica:	( )	Si	( )	No
Videograbación:	( )	Si	( )	No
Por escrito:	( )	Si	( )	No
Otros:				

Observaciones

3. Recolección o levantamiento:

a) Descripción de la forma en que se realizó:
b) Medidas tomadas para preservar la integridad del indicio o evidencia:

4. Entrega de indicios o evidencias:			
Fecha:		Hora:	
Nombre de la persona que entrega:			
Cargo de la persona que entrega:			
Tipo de indicio o evidencia			
Tipo de embalaje y condiciones en que se entrega el embalaje			
Documentos			
Observaciones al estado en que se reciben los indicios o evidencias			
Nombre y firma de quién entrega		Nombre y firma de quién recibe	

- **FORMATO DE RECUPERACIÓN DEL INCIDENTE**

1. Continuidad en la operación				
El sistema de tratamiento continua con su operación después del incidente	( )	Si	( )	No
En caso de "No" indicar las causas:				

Personal designado para dar seguimiento a la recuperación del incidente		
Iniciales	Nombre completo	Puesto

2. Tiempos:		
Fecha en que fue detectado	Fecha en que fue atendido por el equipo de respuesta a incidentes	Fecha en que fue cerrado
Hora en que fue detectado	Hora en que fue atendido por el equipo de respuesta a incidentes	Hora en que fue cerrado

3. Monitoreo:
Describir las acciones que se realizarán para monitorizar las medidas implementadas:
Describir las herramientas para el monitoreo de las medidas implementadas (si es el caso):

Nombre y firma de quién realiza la recuperación	Nombre y firma de quién validó la recuperación

- **FORMATO DE RECUPERACIÓN DEL INCIDENTE**

1. Descripción:	
Fecha:	
Sistema de tratamiento afectado:	
Información/datos personales involucrados en el incidente:	
Resumen Ejecutivo	
Acciones realizadas	
Impacto a la organización/institución	

REGISTROS DE COMUNICACIÓN SOBRE EL INCIDENTE

Comunicación entre A-B					
Fecha:		Hora:		Método:	
			Iniciador		Receptor
Nombre:					
Puesto/Área:					
Organización/Institución a la que pertenece:					
Información de contacto:					
Detalles					

Comunicación entre B-C					
Fecha:		Hora:		Método:	
			Iniciador		Receptor
Nombre:					
Puesto/Área:					
Organización/Institución a la que pertenece:					
Información de contacto:					
Detalles					

Comunicación entre C-D					
Fecha:		Hora:		Método:	
			Iniciador		Receptor
Nombre:					
Puesto/Área:					
Organización/Institución a la que pertenece:					
Información de contacto:					
Detalles					