POLITICAS INTERNAS PARA LA GESTIÓN Y TRATAMIENTO DE DATOS PERSONALES CIATEC, A.C.

OBJETIVO

Implementar los principios y deberes en materia de protección de datos personales en los procesos internos de gestión y tratamiento de datos personales del CIATEC A.C., conforme a lo previsto en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) y los Lineamientos de Protección de Datos Personales para el Sector Público.

ÁMBITO DE APLICACIÓN

El presente documento es de aplicación y observancia general y obligatoria para todas las personas servidoras públicas del CIATEC, A.C., que conforme a sus atribuciones realicen tratamiento de datos personales.

DISPOSICIONES GENERALES

1. Se debe realizar el tratamiento de datos personales con base en las atribuciones conferidas a cada una de las áreas del CIATEC, A.C., dentro del marco legal en la materia y del consentimiento de la persona titular.

2. Previo a recabar datos personales, se debe mostrar el aviso de privacidad integral y/o simplificado, según sea el caso; el aviso de privacidad debe encontrarse en un lugar visible.

3. Al momento de recabar datos personales, se deberá hacer del conocimiento de la persona titular la finalidad con la cual se reciben.

4. Las áreas solo deberán tratar los datos personales que resulten estrictamente necesarios para el ejercicio de atribuciones y funciones.

5. Se deberán adoptar las medidas necesarias para mantener exactos, completos, correctos y actualizados los datos personales que se reciban en ejercicio de las atribuciones otorgadas a las áreas del CIATEC, A.C.

6. Es obligación de todas las personas servidoras públicas del CIATEC, A.C. que administren, actualicen o tengan acceso a bases de datos personales, conservar, manejar y mantener de manera estrictamente confidencial dicha información y no revelarla a terceros.

7. Cuando se recaben datos personales de menores de edad se deberá obtener el consentimiento expreso de quien o quienes ejerzan la patria potestad o tutela sobre éstos.

8. Las áreas deberán identificar todos los avisos de privacidad que se requieren, según los tratamientos que realicen.

9. Los avisos de privacidad deberán ser elaborados en sus dos modalidades: simplificado e integral y contener todos los elementos informativos que exige la norma, además de estar redactados de manera clara y sencilla.

10. Las áreas deberán verificar que sus avisos de privacidad simplificados e integrales se difundan en el portal de internet del CIATEC, A.C. y estar disponibles de manera impresa en las instalaciones, en un lugar visible y de fácil consulta por parte de las personas titulares.

PRINCIPIOS, DEBERES Y DEMÁS OBLIGACIONES

- Licitud
- Lealtad
- Consentimiento
- Información
- Proporcionalidad
- Finalidad
- Calidad
- Responsabilidad

Principio de licitud. Los datos personales tienen que ser tratados de manera lícita, esto es, debe sujetarse a las facultades o atribuciones que la normatividad aplicable le otorga.

Principio de lealtad. La obtención de los datos personales no podrá hacerse a través de medios engañosos, ni fraudulentos.

Principio del consentimiento. Como regla general, las áreas que realicen tratamiento de datos personales deberán contar con el consentimiento del titular para el tratamiento de sus datos personales, el cual deberá ir siempre ligado a las finalidades concretas del tratamiento que se informen en el aviso de privacidad.

Principio de información. Las áreas que realizan tratamientos de datos personales se encuentran obligadas a informar a las personas titulares de los datos personales, a través de los avisos de privacidad integral y simplificado, las características principales del tratamiento al que serán sometidos sus datos personales, a fin de que pueda tomar decisiones informadas al respecto.

Principio de proporcionalidad. Las áreas que realicen tratamiento de datos personales deberán tratar solo aquellos datos personales que resulten necesarios, adecuados y relevantes en relación con las finalidades para las cuales se obtuvieron.

Principio de finalidad. Los datos personales sólo pueden ser tratados para cumplir con la finalidad o finalidades que hayan sido informadas a la persona titular en el aviso de privacidad y, en su caso, consentidas por ésta. Se entiende por finalidad del tratamiento, el propósito, motivo o razón por el cual se tratan los datos personales.

Principio de calidad. El principio de calidad significa que, conforme a la finalidad o finalidades para las que se vayan a tratar los datos personales, éstos deben ser:

- EXACTOS. Los datos personales son exactos cuando reflejan la realidad de la situación de su titular, es decir, son verdaderos o fieles.
- COMPLETOS. Los datos personales son completos cuando no falta ninguno de los que se requiera para las finalidades para las cuales se obtuvieron y son tratados, de forma tal que no se cause un daño o perjuicio a su titular.
- PERTINENTES. Los datos personales son pertinentes cuando corresponden efectivamente a su titular.
- ACTUALIZADOS. Los datos personales están actualizados cuando están al día y corresponden a la situación real de su titular.
- CORRECTOS. Los datos personales son correctos cuando cumplen con todas las características anteriores, es decir, son exactos, completos, pertinentes y actualizados.

Principio de responsabilidad. A este principio se le conoce también como el principio de "rendición de cuentas", ya que establece la obligación de los responsables de velar por el cumplimiento del resto de los principios, adoptar las medidas necesarias para su aplicación, y demostrar ante titulares y la autoridad, que cumple con sus obligaciones en torno a la protección de los datos personales.

Deber de confidencialidad. Este deber implica la obligación de guardar secreto respecto de los datos personales que son tratados. Este deber debe cumplirse para evitar causar un daño a su titular. De no ser así, un tercero no autorizado podría tener acceso a determinada información.

Deber de seguridad. Este deber se refiere a la obligación de establecer y mantener medidas de seguridad tanto técnicas, físicas y administrativas, que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado.

ROLES Y RESPONSABILIDADES

Con relación a lo dispuesto en el artículo 33, fracción II de la LGPDPPSO, el responsable deberá establecer y documentar los roles y responsabilidades, así como la cadena de rendición de cuentas de todas las personas que traten datos personales en su organización, conforme al sistema de gestión implementado.

SANCIONES

Serán causas de sanción por incumplimiento de las obligaciones en materia de protección de datos personales, las establecidas en el artículo 163 de la LGPDPPSO:

I. Actuar con negligencia, dolo o mala fe durante la sustanciación de las solicitudes para el ejercicio de los derechos ARCO;

II. Incumplir los plazos de atención para responder las solicitudes para el ejercicio de los derechos ARCO o para hacer efectivo el derecho de que se trate;

III. Usar, sustraer, divulgar, ocultar, alterar, mutilar, destruir o inutilizar, total o parcialmente y de manera indebida datos personales, que se encuentren bajo su custodia o a los cuales tengan acceso o conocimiento con motivo de su empleo, cargo o comisión;

IV. Dar tratamiento, de manera intencional, a los datos personales en contravención a los principios y deberes establecidos en la presente Ley;

V. No contar con el aviso de privacidad, o bien, omitir en el mismo alguno de los elementos a que refiere el artículo 27 de la presente Ley, según sea el caso, y demás disposiciones que resulten aplicables en la materia;

VI. Clasificar como confidencial, con dolo o negligencia, datos personales sin que se cumplan las características señaladas en las leyes que resulten aplicables;

VII. Incumplir el deber de confidencialidad;

VIII. No establecer las medidas de seguridad en los términos que establecen los artículos 31, 32 y 33 de la LGPDPPSO;

IX. Presentar vulneraciones a los datos personales por la falta de implementación de medidas de seguridad;

X. Llevar a cabo la transferencia de datos personales, en contravención a lo previsto en la LGPDPPSO;

XI. Obstruir los actos de verificación de la autoridad.