

# POLITICA DE PROTECCION DE DATOS PARA EL CANAL DE DENUNCIAS

Asociación Tinerfeña de Trisómicos 21

**Asociación Tinerfeña de Trisómicos 21**  
**G38328704**  
**Fecha de realización: 17/09/2024**

## Índice

1. Introducción
2. Ámbito de aplicación
3. Normativa de aplicación
4. Medidas técnicas y organizativas aplicadas al Canal de Denuncias
  - 4.1.- Obligación de contar con Delegado de Protección de Datos (DPD)
  - 4.2.- Deber de Información
  - 4.3.- Encargados del Tratamiento
  - 4.4.- Transferencias Internacionales
  - 4.5.- Confidencialidad y Anonimato. Datos del informante y de terceros
  - 4.6.- Personal Autorizado a Acceder a Datos
  - 4.7.- Plazos de Conservación de Datos (Libro - Registro)
  - 4.8.- Medidas de Seguridad
  - 4.9.- Registro de Actividad del Tratamiento (RAT)
  - 4.10.- Brechas de Seguridad
  - 4.11.- Derechos ARCO+
  - 4.12.- Portal del Cliente

### 1. Introducción

Desde el momento en que la empresa decida llevar a cabo cualquier acción en la que se obtengan o utilicen datos personales debe tener en cuenta la normativa de protección de datos adoptando las medidas necesarias para su cumplimiento.

El presente protocolo recoge las medidas y los requisitos para dar cumplimiento al apartado de protección de datos en la implementación del Canal de Denuncias en su empresa.

### 2. Ámbito de aplicación

Este protocolo y las medidas de seguridad en él contenidas corresponde implantarlas al Responsable del Tratamiento, Asociación Tinerfeña de Trisómicos 21, quien deberá velar por su cumplimiento por parte de toda la organización, personal laboral, y terceros que puedan acceder a datos personales utilizados para la gestión del Canal de Denuncias implantado en la empresa.

Es IMPORTANTE destacar que este protocolo describe únicamente las medidas a tomar en materia de PROTECCIÓN DE DATOS en el Canal de Denuncias. En ningún caso se establecen las medidas para la implementación del Canal de Denuncias en su totalidad.

### 3. Normativa de aplicación

Como norma general, y al margen de aquellas normativas sectoriales que sean de aplicación dada la actividad

profesional del responsable, serán de aplicación al tratamiento de los datos personales las siguientes normativas:

- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).
- Ley Orgánica de Protección de datos y garantía de derechos digitales, Ley 3/2018 de 5 de diciembre.

Además, para la implantación y gestión del Canal de Denuncias se deben tener en cuenta, según la actividad profesional del responsable, alguna o todas las siguientes normativas:

- Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción.
- Ley Orgánica 3/2007, de 22 de marzo, para la igualdad efectiva de mujeres y hombres.
- Ley Orgánica 8/2021, de 4 de junio, de protección integral a la infancia y la adolescencia frente a la violencia.

#### **4. Medidas técnicas y organizativas aplicadas al Canal de Denuncias**

Estas medidas de responsabilidad activa, se deben aplicar con anterioridad al inicio del tratamiento y también cuando se esté desarrollando.

##### **4.1.- Obligación de contar con Delegado de Protección de Datos (DPD)**

Para promover el cumplimiento normativo en materia de protección de datos durante el proceso de gestión de la información recibida a través del Canal de Denuncias es obligatorio contar con un Delegado de Protección de Datos designado en su empresa.

Es importante que, antes de implementar el Canal de Denuncias en su empresa, informen a su Delegado de Protección de Datos para que pueda dar las recomendaciones necesarias para el cumplimiento de la normativa de protección de datos.

##### **4.2.- Deber de Información:**

- Cuando se reciba una denuncia, se debe entregar la información sobre el tratamiento de los datos que conlleva la formulación de una denuncia a:

- Denunciantes

- Denunciados

- Testigos

- Terceros afectados

Además, a los denunciantes se les debe informar, de forma expresa, de que su identidad será en todo caso reservada, que no se comunicará a las personas a las que se refieren los hechos relatados ni a terceros.

La información deberá entregarse en un plazo razonable y que no exceda de un mes, pudiendo ampliarse a tres meses en caso de una investigación prolongada.

Existen diferentes medios para dar la información de protección de datos a los **Denunciantes**, siempre según el medio de recepción de la denuncia:

- En caso de utilizar un **Canal de Denuncias digital (formulario web)**:

1.- Se debe añadir bajo el formulario una casilla para la aceptación de la Política de Privacidad de Asociación Tinerfeña de Trisómicos 21. Esta casilla no podrá estar pre-marcada y el texto -Política de Privacidad – deberá estar enlazado a al texto de Política de Privacidad de la web.

2.- Se debe facilitar la - Información Básica de Protección de Datos del Canal de Denuncias - bajo el formulario habilitado. El texto a utilizar se encuentra en su Portal del Cliente.

- En caso de utilizar un **correo electrónico como medio para la presentación de denuncias**:

1.- Se debe implementar una respuesta automática que contenga la - Información Básica de Protección de Datos del Canal de Denuncias -. El texto a utilizar se encuentra en su Portal del Cliente.

2.- Se debe conservar esta respuesta mientras se conserve la denuncia para poder demostrar el cumplimiento en cuanto al deber de información de protección de datos.

Este medio para la presentación de denuncias no es recomendable debido a la falta de confidencialidad, la inseguridad de las comunicaciones, la supervisión limitada y la dificultad para documentar.

- En caso de utilizar **sistema de mensajería de voz o llamada telefónica como medio de presentación de denuncias**:

1.- Se debe facilitar la - Información Básica de Protección de Datos del Canal de Denuncias – mediante una locución.

2.- Se debe grabar la llamada para documentar la denuncia en formato seguro, duradero y accesible.

3.- Se debe solicitar el consentimiento del informante para grabar la llamada preguntando explícitamente si consiente la grabación o no. Este consentimiento deberá poder demostrarse de algún modo, por lo que se tendrá que utilizar un medio para ello, por ejemplo, grabando la respuesta a la pregunta: "¿Está de acuerdo en que se grabe esta conversación en los términos que le hemos expuesto?", o marcando un número para dar su consentimiento y otro para rechazar la grabación, etc.

Este medio para la presentación de denuncias no es recomendable debido a la falta de confidencialidad, la supervisión limitada y la dificultad para documentar.

Si el informante decide no dar el consentimiento para la grabación no podrá ser documentada y, por tanto, el sistema quedaría invalidado.

- En caso de que el **informante decida realizar la denuncia mediante reunión presencial**:

1.- Se debe facilitar la - Información Básica de Protección de Datos del Canal de Denuncias – entregando un documento para su firma.

2.- Se debe documentar la denuncia comunicada verbalmente de alguna de las maneras siguientes, previo consentimiento del informante:

a) mediante una grabación de la conversación en un formato seguro, duradero y accesible, o b) a través de una transcripción completa y exacta de la conversación realizada por el personal responsable de tratarla.

Este medio para la presentación de denuncias no es recomendable debido a la falta de confidencialidad, la supervisión limitada y la dificultad para documentar pero el informante tiene derecho a dar la información mediante una reunión presencial.

- En el caso de las personas **Denunciadas, Testigos y terceros Afectados** también se le entregará la información sobre el tratamiento de sus datos. Se utilizará un documento específico para ello que puede encontrar en su Portal del Cliente.

- Se debe comunicar a los trabajadores la existencia del Canal de Denuncias y su Reglamento (documento creado por Asociación Tinerfeña de Trisómicos 21). En dicho Reglamento de Canal de Denuncias se debe incluir la información de protección de datos. Se utilizará un texto específico para ello que puede encontrar en su Portal del Cliente.

En todo caso, se debe añadir la información adicional de protección de datos relativa al Canal de Denuncias en la Política de Privacidad de la empresa.

#### **4.3.- Encargados del Tratamiento**

Un Encargado de Tratamiento de datos se define como aquella persona física o jurídica, autoridad pública u organismo que brinda un servicio que conlleva el tratamiento de datos personales por cuenta del Responsable del Tratamiento.

- Ejemplos de Encargados del Tratamiento en el Canal de Denuncias:

El proveedor del aplicativo para la gestión del Canal de Denuncias, el proveedor de correo electrónico utilizado como medio para realizar denuncias, el servicio de alojamiento de los datos, etc.

- Garantías de cumplimiento de los Encargados del Tratamiento:

El Responsable del Tratamiento debe elegir Encargados del Tratamiento que ofrezcan garantías suficientes respecto a la implantación y el mantenimiento de las medidas técnicas y organizativas apropiadas, de acuerdo con lo establecido en el RGPD, y que garanticen la protección de los derechos de las personas afectadas. Existe, por tanto, un deber de diligencia en la elección del Responsable.

Para demostrar que el Encargado ofrece garantías suficientes, el RGPD prevé que la adhesión a códigos de conducta o la posesión de un Certificado de Protección de Datos pueden servir como mecanismos de prueba. También puede encontrar un Cuestionario de Valoración de Garantías del Encargado en su Portal de Cliente.

- Contratos de Encargo del Tratamiento:

El tratamiento de los datos personales por cuenta de terceros distintos del Responsable del Tratamiento deberá estar regulado por la existencia de un contrato. Podrán encontrar estos contratos de encargo del tratamiento entre los documentos disponibles en su Portal del Cliente.

#### **4.4.- Transferencias Internacionales**

Las transferencias internacionales de datos suponen un flujo de datos personales desde el territorio español a destinatarios establecidos en países fuera del Espacio Económico Europeo (los países de la Unión Europea más Liechtenstein, Islandia y Noruega)

- - Los países fuera del Espacio Económico Europeo (EEE) no siempre cumplen el nivel de protección de datos adecuado, por lo que, en caso de darse transferencias internacionales de datos se deberá verificar que se cumple con las garantías adecuadas.

- Para verificar el cumplimiento de los diferentes territorios puede consultar este link: [Garantías para las transferencias de datos personales a terceros países u organizaciones internacionales](#)

#### **4.5.- Confidencialidad y anonimato. Datos del informante y de terceros.**

Se debe preservar la identidad del informante y de las personas afectadas. Esto implica implementar todas las medidas reforzadas de seguridad y confidencialidad de la información.

- Se permiten sistemas de denuncias anónimas pero, en el caso de que esta no lo sea, la información del

informante debe quedar a salvo, este tiene derecho a que su identidad no sea revelada a terceras personas y a que no se facilite su identificación al denunciado.

- Denuncia a través de un formulario habilitado para ello: se debe establecer como – opcional - la identificación del informante. Es decir, no se debe solicitar en el formulario como datos obligatorios su nombre, apellidos, documento identificativo, correo electrónico, etc. El sistema debe dar la posibilidad de realizar la denuncia de manera totalmente anónima.

- Denuncia a través de un correo electrónico habilitado para ello: en este caso no es posible realizar la denuncia de forma totalmente anónima ya que se puede identificar al denunciante a través del correo electrónico desde que se envíe la información. Este medio para la presentación de denuncias no es el más recomendado debido a la imposibilidad de conservar el anonimato del denunciante.

- Denuncia a través de buzón en llamada telefónica: Este medio para la presentación de denuncias no es el más recomendado debido a la imposibilidad de conservar el anonimato del denunciante.

- Denuncia en reunión solicitada: Este medio para la presentación de denuncias no es el más recomendado debido a la imposibilidad de conservar el anonimato del denunciante.

- La identidad del resto de personas afectadas y terceros que se mencionen en la denuncia debe ser preservada.

- La identidad del informante solo podrá ser comunicada a la Autoridad judicial, al Ministerio Fiscal o a la autoridad administrativa competente en el marco de una investigación penal, disciplinaria o sancionadora. En caso de darse alguna de las comunicaciones mencionadas, se trasladará al informante antes de revelar su identidad, salvo que dicha información pudiera comprometer la investigación o el procedimiento judicial. La comunicación se realizará estableciendo todas las salvaguardas necesarias.

- Si el personal no responsable del tratamiento de denuncias recibe una comunicación por un canal que no sea el establecido para ello debe remitir dicha comunicación inmediatamente al Responsable del Sistema. El receptor de la comunicación debe mantener la confidencialidad.

#### **4.6.- Personal autorizado a acceder a datos**

- El acceso a los datos personales contenidos en el Canal de Denuncias quedará limitado, dentro del ámbito de sus competencias y funciones, exclusivamente a:

a) El Responsable del Sistema y a quien lo gestione directamente.

b) El responsable de recursos humanos, solo cuando pudiera proceder la adopción de medidas disciplinarias contra un trabajador.

c) El responsable de los servicios jurídicos, si procediera la adopción de medidas legales en relación con los hechos relatados en la comunicación.

d) Los encargados del tratamiento que eventualmente se designen.

e) El Delegado de Protección de Datos.

- Será lícito el tratamiento de los datos por otras personas, o incluso su comunicación a terceros, cuando resulte necesario para la adopción de medidas correctoras en la entidad o la tramitación de los procedimientos sancionadores o penales que, en su caso, procedan.

- La Autoridad judicial competente, a petición razonada mediante auto, y en el marco de un procedimiento judicial y bajo la tutela de aquella, podrá accederse total o parcialmente al contenido del libro-registro de las informaciones recibidas e investigaciones internas a que hayan dado lugar.

#### **4.7.- Plazos de Conservación (Libro – Registro)**

Se debe contar con un libro-registro de las informaciones recibidas y de las investigaciones internas a que hayan dado lugar.

- Los datos personales relativos a las informaciones recibidas y a las investigaciones internas solo se conservarán durante el período que sea necesario y proporcionado. En ningún caso podrán conservarse los datos por un período superior a diez años

- Si se acreditara que la información facilitada no es veraz, deberá procederse a su inmediata supresión, salvo que dicha falta de veracidad pueda constituir un ilícito penal, en cuyo caso se guardará la información por el tiempo necesario durante el que se tramite el procedimiento judicial.

- Los datos personales de las denuncias para las que no proceda su investigación, por no estar fundamentadas, deberán borrarse o anonimizarse transcurridos tres meses desde su recepción.

- Si la información recibida contuviera datos personales incluidos dentro de las categorías especiales de datos, se procederá a su inmediata supresión, sin que se proceda al registro y tratamiento de los mismos.

Las comunicaciones recibidas por otros canales diferentes al Canal de Denuncias, deberán eliminarse inmediatamente después de informar al Responsable del Sistema.

#### **4.8.- Medidas de seguridad**

Se deben Implantar las medidas de seguridad técnicas y organizativas necesarias para garantizar la seguridad de los datos tratados en la gestión del Canal de Denuncias. De manera enunciativa más no limitativa se debe:

- Los trabajadores y terceros con autorización a acceder a la información relativa a las denuncias deberán ser informados acerca del tratamiento de datos personales de manera segura y sobre su obligación de confidencialidad.
- Realizar copias de seguridad.
- Cifrado de datos (en tránsito y reposo).
- Establecer política contraseñas.
- Control de accesos. Cada acceso de un usuario a datos deberá quedar registrado.
- Medidas esenciales de seguridad de dispositivos utilizados para el acceso al Canal de Denuncias (actualizaciones de sistema y antivirus, conexión a redes privadas, control de accesos, bloqueo de manera automática).

#### **4.9.- Registro de Actividades del Tratamiento (RAT)**

Se debe elaborar el Registro de Actividad del Tratamiento del Canal de Denuncias.

#### **4.10.- Brechas de Seguridad**

Si se detecta alguna Brecha de Seguridad se debe informar a su Delegado de Protección de Datos inmediatamente y consultar el Protocolo para la Gestión de Brechas de Seguridad.

#### **4.11.- Derechos ARCO+**

En caso de que un usuario del Canal de Denuncias quiera ejercitar alguno de sus derechos de protección de datos, podrá hacerlo solicitando el formulario para el ejercicio de sus derechos o utilizar cualquier otro medio, como correo electrónico o presentar presencialmente un escrito propio solicitando el ejercicio de un derecho con sus propias palabras. Los formularios para el ejercicio de los derechos puede encontrarlos en su Portal del Cliente, apartado Interesados.

Para la respuesta al ejercicio de derechos ARCO+, puede consultar el Protocolo de Respuesta de Ejercicios de Derechos ARCO+. En todo caso, le recomendamos que siempre informe a Nubelia, lo antes posible.

#### **4.12.- Portal del Cliente**

Desde el Portal del Cliente de Nubelia puede acceder a:

- Los documentos necesarios para dar la información de protección de datos a los interesados:

- Documento 2031:

- Si se recibe la denuncia mediante una reunión presencial se debe entregar este documento al denunciante para su firma.

- Si se recibe una denuncia (por cualquier medio) se debe entregar la información de protección de datos a denunciados, testigos y terceros. Si se prefiere entregar esta información en papel, puede utilizar este documento que el interesado debe firmar.

- Documento 2032:

- Si se recibe la denuncia mediante un correo habilitado para ello se debe enviar este documento al denunciante y conservar prueba de envío.

- Si se recibe una denuncia (por cualquier medio) se debe entregar la información de protección de datos a denunciados, testigos y terceros. Si se prefiere entregar esta información mediante correo electrónico, se enviará este texto y se conservará prueba de envío.

- Documento 2033:

Texto de protección de datos para añadir en el Reglamento del Canal de Denuncias creado y publicitado por Asociación Tinerfeña de Trisómicos 21

- La Política de Privacidad para añadir en la web y el texto a añadir bajo el formulario web habilitado como Canal de Denuncias (en caso de utilizar este medio).

- Los Contratos de Encargo del Tratamiento para formalizar con los prestadores de servicios con acceso a datos y el modelo de Cuestionario para la Valoración de las Garantías del Encargado.

- Las cláusulas de confidencialidad para las personas trabajadoras y terceros con autorización de acceso al Canal de Denuncias (incluidas en el Compromiso de Trabajadores y en los Contratos de Encargo del Tratamiento).

- El Registro de Actividad del Tratamiento del Canal de Denuncias.

- El Protocolo para la Gestión de Brechas de Seguridad.

- El Protocolo de Respuesta de Ejercicios de Derechos ARCO+.