# PROTOCOLO MANEJO RESPONSABLE DE DATOS DEL MINISTERIO DE TRABAJO Y SEGURIDAD SOCIAL

El Ministerio de Trabajo y Seguridad Social (MTSS) cuenta con una bases de datos en la que se resguardan los datos personales de las personas trabajadoras, pensionados, organizaciones sociales y el sector empresarial, que sirven de base para tener actualizado el nivel de desempleo o empleabilidad y la seguridad social que existe a nivel nacional, dichos datos de carácter personal son recopilados con fines determinados, explícitos y legítimos, y no serán tratados posteriormente de manera incompatible con los fines, para los cuales fueron creados.

## Disposiciones Legales de Aplicación

La Ley de Protección de Datos en Costa Rica, se encuentra regulada bajo la Ley No. 8968 *Protección de la Persona frente al tratamiento de sus datos personales* del 5 de noviembre de 2011; la cual fue Reglamentada bajo el Decreto Ejecutivo 37554, "*Reglamento a la Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales"* en fecha 5 de marzo de 2013, y reformado mediante Decreto Ejecutivo 40008 l *Reglamento a la Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales*, la cual entró en vigencia el 6 de diciembre de 2016.

La Ley faculta a las instituciones públicas, a utilizar las bases de datos para cumplir sus funciones. En sus artículos 6, 7 y 11 se indica lo siguiente:

ARTÍCULO 6.- Principio de calidad de la información:

Solo podrán ser recolectados, almacenados o empleados datos de carácter personal para su tratamiento automatizado o manual, cuando tales datos sean actuales, veraces, exactos y adecuados al fin para el que fueron recolectados.

1. Actualidad: Los datos de carácter personal deberán ser actuales. El responsable de la base de datos eliminará los datos que hayan dejado de ser pertinentes o necesarios, en razón de la finalidad para la cual fueron recibidos y registrados. En ningún caso, serán conservados los datos personales que puedan afectar, de cualquier modo, a su titular, una vez transcurridos diez años desde la fecha de ocurrencia de los hechos registrados, salvo disposición normativa especial que disponga otra cosa. En caso de que sea necesaria su conservación, más allá del plazo estipulado, deberán ser desasociados de su titular.

2. Veracidad: Los datos de carácter personal deberán ser veraces. La persona responsable de la base de datos está obligado a modificar o suprimir los datos que falten a la verdad. De la misma manera, velará por que los datos sean tratados de manera leal y lícita.

3. Exactitud: Los datos de carácter personal deberán ser exactos. La persona responsable de la base de datos tomará las medidas necesarias para que los datos inexactos o incompletos, con respecto a los fines para los que fueron recogidos o para los que fueron tratados posteriormente, sean suprimidos o rectificados. Si los datos de carácter personal registrados resultan ser inexactos en todo o en parte, o incompletos, serán eliminados o sustituidos de oficio por la persona responsable de la base de datos, por los correspondientes datos rectificados, actualizados o complementados. Igualmente, serán eliminados si no media el consentimiento informado o está prohibida su recolección.

4. Adecuación al fin: Los datos de carácter personal serán recopilados con fines determinados, explícitos y legítimos, y no serán tratados posteriormente de manera incompatible con dichos fines. No se considerará incompatible el tratamiento posterior de datos con fines históricos, estadísticos o científicos, siempre y cuando se establezcan las garantías oportunas para salvaguardar los derechos contemplados en esta ley. Las bases de datos no pueden tener finalidades contrarias a las leyes ni a la moral pública.

ARTÍCULO 7.- Derechos que le asisten a la persona. Se garantiza el derecho de toda persona al acceso de sus datos personales, rectificación o supresión de estos y a consentir la cesión de sus datos. La persona responsable de la base de datos debe cumplir lo solicitado por la persona, de manera gratuita, y resolver en el sentido que corresponda en el plazo de cinco días hábiles, contado a partir de la recepción de la solicitud.

1. Acceso a la información: La información deberá ser almacenada en forma tal que se garantice plenamente el derecho de acceso por la persona interesada. El derecho de acceso a la información personal garantiza las siguientes facultades del interesado:

    a) Obtener en intervalos razonables, según se disponga por reglamento, sin demora y a título gratuito, la confirmación o no de la existencia de datos suyos en archivos o bases de datos. En caso de que sí existan datos suyos, estos deberán ser comunicados a la persona interesada en forma precisa y entendible.

    b) Recibir la información relativa a su persona, así como la finalidad con que fueron recopilados y el uso que se le ha dado a sus datos personales. El informe deberá ser completo, claro y exento de

codificaciones. Deberá estar acompañado de una explicación de los términos técnicos que se utilicen.

c) Ser informado por escrito de manera amplia, por medios físicos o electrónicos, sobre la totalidad del registro perteneciente al titular, aun cuando el requerimiento sólo comprenda un aspecto de los datos personales. Este informe en ningún caso podrá revelar datos pertenecientes a terceros, aun cuando se vinculen con la persona interesada, excepto cuando con ellos se pretenda configurar un delito penal.

d) Tener conocimiento, en su caso, del sistema, programa, método o proceso utilizado en los tratamientos de sus datos personales. El ejercicio del derecho al cual se refiere este artículo, en el caso de datos de personas fallecidas, le corresponderá a sus sucesores o herederos.

2.- Derecho de rectificación: Se garantiza el derecho de obtener, llegado el caso, la rectificación de los datos personales y su actualización o la eliminación de estos cuando se hayan tratado con infracción a las disposiciones de la presente ley, en particular a causa del carácter incompleto o inexacto de los datos, o hayan sido recopilados sin autorización del titular. Todo titular puede solicitar y obtener de la persona responsable de la base de datos, la rectificación, la actualización, la cancelación o la eliminación y el cumplimiento de la garantía de confidencialidad respecto de sus datos personales. El ejercicio del derecho al cual se refiere este artículo, en el caso de datos de personas fallecidas, le corresponderá a sus sucesores o herederos.

ARTÍCULO 11.- Deber de confidencialidad

La persona responsable y quienes intervengan en cualquier fase del tratamiento de datos personales están obligadas al secreto profesional o funcional, aun después de finalizada su relación con la base de datos. La persona obligada podrá ser relevado del deber de secreto por decisión judicial en lo estrictamente necesario y dentro de la causa que conoce.

**Administración y uso de la información**

La instancia encargada de la elaboración del Protocolo del manejo responsable de datos del Ministerio de Trabajo y Seguridad Social es el Departamento de Tecnologías de la Información y comunicación DTIC.

El alcance del presente Protocolo y sus recomendaciones se extiende a toda la información contenida en las bases de datos y archivos electrónicos que por su naturaleza estén contenidos en estas, que existen en el Ministerio de Trabajo y Seguridad Social.

**Objetivo**

Establecer los lineamientos que orienten los procedimientos establecidos en el MTSS y las actuaciones de todos y cada uno de los colaboradores de las actividades de la Bases de Datos en consecuencia a la recolección, actualización, almacenamiento, uso, circulación, supresión y, en general, toda actividad que implique el tratamiento de los datos personales a nivel tecnológico.

**Alcance**

Todos los procesos, operaciones y personal del MTSS que participe en cualquiera de las etapas de recolección, conocimiento, custodia y tratamiento de datos personales a nivel tecnológico.

**Clasificación de los Datos**

Datos personales: cualquier dato relativo a una persona física identificada o identificable.

Datos personales de acceso irrestricto: los contenidos en bases de datos públicas de acceso general, según dispongan leyes especiales y de conformidad con la finalidad para la cual estos datos fueron recabados.

Datos personales de acceso restringido: los que, aun formando parte de registros de acceso al público, no son de acceso irrestricto por ser de interés solo para su titular o para la Administración Pública.

Datos sensibles: información relativa al fuero íntimo de la persona, como por ejemplo los que revelen origen racial, opiniones políticas, convicciones religiosas o espirituales, condición socioeconómica, información biomédica o genética, vida y orientación sexual, entre otros.

**Bases de Datos Administradas por MTSS**

El MTSS está autorizado para administrar todas las bases de datos necesarias para el desarrollo de su actividad para los servicios brindados, para lo cual, su tratamiento se sujetará a lo establecido en el presente protocolo que contiene las políticas, normas,

reglas, pautas y procedimientos internos establecidos para garantizar el buen uso de las bases de datos y su integridad.

El MTSS administrará preferentemente las siguientes bases de datos, pero no se limitará a las mismas:

a) Datos personales personas trabajadores y de patronos.

b) Datos de organizaciones sociales.

c) Datos de Pensionados.

d) Cualquier otro que sea considerado relevante para la continuidad del negocio.

El MTSS podrá crear otras bases de datos actuando como responsable del tratamiento o interviniendo como encargado del mismo, para lo cual, previo a su tratamiento se verificará el cumplimiento de todos y cada uno de las estipulaciones consagradas en el presente protocolo.

**Creación de bases de datos**

El DTIC será el encargado de diseñar física y lógicamente las bases de datos, que utilizarán los sistemas de información que sean desarrollados internamente en el MTSS.

El Departamento de DTIC permitirá la creación de bases de datos a empresas contratadas para este fin o para el desarrollo de sistemas de información, siempre que se desarrollen en apego a los estándares e implementación de las mejores prácticas en cuanto al diseño físico y lógico, y que entreguen la documentación técnica requerida del diseño de la base de datos así como cualquier otro solicitado por el DTIC referente a esta.

En la creación de nuevas bases de datos se deberá generar la documentación necesaria y suficiente, que permita comprender su estructura física y lógica, así como su contenido.

En la definición de nomenclatura para las bases de datos, deberá estar apegada a los estándares y recomendaciones del fabricante del motor de la base de datos y en casos donde sea desarrollada por una empresa contratada deberá ser validada por el DTIC.

EL DTIC como parte de las mejores prácticas a implementar hará uso de una herramienta para el modelado de datos, creación y generación de base de datos, para lo cual debe adquirirse la respectiva licencia y la capacitación para su manejo.

**Migración de información de bases de datos**

Toda migración de base de datos deberá ser realizada por personal técnico capacitado interno o personal externo contratado para este fin, el cual deberá ser supervisado por un profesional del DTIC.

Antes de cualquier proceso de migración se deberán realizar los respaldos respectivos, así como realizar previamente una prueba de la migración en un servidor de pruebas, para garantizar que el proceso de migración funciona correctamente.

En las actividades de migración de información a bases de datos, se deberá documentar el procedimiento a realizar, así como dejar documentado en una bitácora todo lo realizado para futuras migraciones.

**Instalación de bases de datos**

Toda instalación de base de datos deberá ser realizada por el personal técnico capacitado del DTIC, o en su defecto por personal de empresas contratadas para estos efectos, bajo la supervisión DTIC.

Antes de cualquier instalación deberán realizarse los respaldos respectivos para evitar accidentes y garantizar la recuperación de la base de datos.

Para la instalación de bases de datos se deberá seguir las recomendaciones brindadas por el DTIC para con el fin de implementar las mejores prácticas para el rendimiento de las bases de datos y prevenir que se den atrasos o complicaciones, así como dejar documentado en una bitácora todo lo realizado.

**Administración y mantenimiento de bases de datos**

Todo mantenimiento a las bases de datos deberá ser realizado por personal técnico capacitado interno o externo, quienes deberán ser supervisados por el profesional responsable de esa tarea del DTIC y deberán apegarse a las recomendaciones que este considere oportunas brindar.

Antes de cualquier proceso de mantenimiento a la base de datos, se deberán realizar los respaldos respectivos para estar prevenidos contra cualquier accidente que se pudiera presentar.

Todo cambio o ajuste hecho en el proceso de mantenimiento, se deberá dejar documentado en una bitácora para efectos de control y seguimiento.

**Tiempos de almacenamiento de información en bases de datos**

El Departamento de TI o cualquier empresa contratada para este fin, deberá, garantizar la conservación permanente de toda la información almacenada en las bases de datos

de los servidores, que esté directa o indirectamente relacionada con las actividades del MTSS.

La información deberá ser conservada durante el período que se defina en la tabla de plazos de conservación, labor en la cual tendrá concurso el Archivo Central de la Institución, y los respaldos por periodo de tiempo establecido por el DTIC de acuerdo a la capacidad de almacenamiento existente.

Toda transacción que se ejecute en las bases de datos, dejará las pistas adecuadas de auditoría, para poder ejercer un control adecuado, de todas las modificaciones que se hagan en éstas mediante el uso de bitácoras.

Deberán de mantenerse y aplicarse sistemas de respaldos para todas las bases de datos del MTSS, con el fin de garantizar la disponibilidad de la de información y su conservación.

Deberán existir planes de recuperación de la información de las bases de datos, para garantizar la continuidad del servicio que se presta por medio de los sistemas de información.

**Responsable de Bases de Datos.**

Responsable de la base de datos: persona física o jurídica que administre, gerencie o se encargue de la base de datos, ya sea esta una entidad pública o privada, competente, con arreglo a la ley, para decidir cuál es la finalidad de la base de datos, cuáles categorías de datos de carácter personal deberán registrase y qué tipo de tratamiento se les aplicarán.

**Tratamiento de datos.**

Cualquier operación o conjunto de operaciones, efectuadas mediante procedimientos automatizados o manuales y aplicadas a datos personales, tales como la recolección, el registro, la organización, la conservación, la modificación, la extracción, la consulta, la utilización, la comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a estos, el cotejo o la interconexión, así como su bloqueo, supresión o destrucción, entre otros.

**Seguridad en bases de datos.**

Todo acceso a las bases de datos del MTSS deberá contar con los mecanismos adecuados y controlados, que garanticen su seguridad, su integridad y la confidencialidad de la información almacenada.

Toda transacción que se ejecute en las bases de datos, dejará las pistas adecuadas de auditoría, para poder ejercer un control adecuado, de todas las modificaciones que se hagan en éstas mediante el uso de bitácoras.

Deberán de mantenerse y aplicarse sistemas de respaldos para todas las bases de datos del MTSS, con el fin de garantizar su conservación.

Se deberá cumplir con los establecido en las políticas de seguridad de la información referentes al almacenamiento y seguridad de las bases de datos.

**Seguridad de acceso a bases de datos.**

El DTIC velará porque toda base de datos que sea instalada, cuente con los controles de seguridad que garanticen la confiabilidad de la información.

Los códigos de acceso de los usuarios de las bases de datos deberán apegarse a las políticas de seguridad de la información del DTIC.

Mediante una solicitud el administrador de la base de datos podrá asignar la clave de acceso al usuario cuando sea requerido.

El DTIC deberá contemplar el bloqueo de claves a usuarios cuando considere que estos accesos ya no son requeridos.

Se deberán implementar por parte de los encargados de las bases de datos controles para verificar que todos los respaldos de información efectuados, se encuentren almacenados en medios de almacenamiento externos al servidor de bases de datos o en la nube.

Los encargados internos y externos de base de datos, deberán de firmar un contrato que garantice la confidencialidad de los datos contenidos en las bases de datos.

JORGE VIQUEZ LOPEZ (FIRMA)

Firmado digitalmente por JORGE VIQUEZ LOPEZ (FIRMA)
Fecha: 2020.04.23 08:32:24 -06'00'

Jorge Víquez López
**Depto. Tecnologías de Información y Comunicaciones**