TABLA DE CONTENIDO

[MEDIDAS DE SEGURIDAD 2](#_Toc523928837)

[1. OBJETIVO 2](#_Toc523928838)

[2. ALCANCE 2](#_Toc523928839)

[3. DEFINICIONES 2](#_Toc523928840)

[4. CLASIFICACIÓN DE LAS MEDIDAS DE SEGURIDAD 7](#_Toc523928841)

[5. TIPOS DE DATOS Y NIVEL DE SEGURIDAD 7](#_Toc523928842)

[6. CLASIFICACIÓN BASES DE DATOS 8](#_Toc523928843)

[7. MEDIDAS DE SEGURIDAD 8](#_Toc523928844)

[7.1. NIVEL BAJO 8](#_Toc523928845)

[7.2. NIVEL MEDIO 9](#_Toc523928846)

[7.3. NIVEL ALTO 12](#_Toc523928847)

[8. FUNCIONES DEL OFICIAL DE PROTECCIÓN DE DATOS PERSONALES 12](#_Toc523928848)

# MEDIDAS DE SEGURIDAD

## OBJETIVO

El objetivo del presente documento, es definir las Medidas de Seguridad que deben adoptarse para la Protección de Datos Personales según el Tipo de Base de Datos y la Naturaleza de los mismos, en aras de dar cabal cumplimiento a la Ley Estatutaria No. 1581 de 2012, su Decreto Reglamentario 1074 de 2015 (Capítulo 25) y demás normas que rigen la Protección de Datos Personales, o aquellas que las complementen, sustituyan, modifiquen o deroguen.

## ALCANCE

Esta Guía es aplicable tanto a la Universidad Católica de Manizales, en calidad de Responsable del Tratamiento y a sus empleados directos e indirectos (en adelante “Operativos”), como a todas aquellas terceras personas naturales o jurídicas que realicen un Tratamiento sobre Datos Personales de los Titulares que comprenden los Grupos de Interés del Responsable del Tratamiento, por Encargo de éste.

## DEFINICIONES

Para los efectos de esta Guía, se entenderá por:

**ADOLESCENTE:** Personas entre 12 y 18 años de edad (Código de la Infancia y de la Adolescencia, artículo 3).

**BASE DE DATOS**: Conjunto organizado de datos personales físico o electrónico (digital) que sea objeto de Tratamiento manual o automatizado.

**CICLO DE VIDA DEL DATO:** Etapas por las que pasan los Datos Personales, desde su recolección, hasta la disposición final de los mismos.

**DATOS PERSONALES**: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. La naturaleza de los Datos Personales puede ser pública, semiprivada, privada o sensible.

|  |  |
| --- | --- |
| **Clases de Datos Personales** | **Ejemplos** |
| **Datos de Identificación** | Datos generales de identificación de la persona, familiares, beneficiarios o terceros. Ej: Nombre, apellido, tipo de identificación, número de identificación, fecha y lugar de expedición, nombre, estado civil, sexo, etc. |
| **Datos específicos de Identificación** | Firma, nacionalidad, datos de familia, firma electrónica, otros documentos de identificación, lugar y fecha de nacimiento o muerte, edad, etc. |
| **Datos Biométricos** | Huella, ADN, iris, Geometría facial o corporal, fotografías, videos, fórmula dactiloscópica, voz, etc. |
| **Datos de contacto empresariales o profesionales** | Dirección, teléfono, correo electrónico, etc. |
| **Datos de contacto personales** | Domicilio, teléfono, correo electrónico, etc. |
| **Datos órdenes para procedimientos médicos** | Órdenes y relación de pruebas complementarias como laboratorio, imagen, endoscópicas, patológicas, estudios, etc. NO INCLUYE RESULTADOS NI DIAGNÓSTICOS. |
| **Datos Resultados y diagnósticos médicos** | Resultados de pruebas, laboratorios, estudios, diagnósticos médicos, generales o especializados, psicológicos o psiquiátricos, medicamentos y/o tratamientos médicos o terapéuticos de cualquier tipo, etc. |
| **Datos de Asociación** | Datos relacionados con la pertenencia a sindicatos, organizaciones sociales, de derechos humanos, religiosas, políticas |
| **Datos sexualidad** | Datos orientación sexual y preferencias sexuales |
| **Datos de Origen** | Datos de origen étnico-racial |
| **Datos de población vulnerable** | Personas de la tercera edad o menores de 18 años en condición de pobreza, personas con limitaciones sicomotoras, auditivas y visuales en condiciones de pobreza, personas víctimas de la violencia, personas en situación de desplazamiento forzado por violencia, madres gestantes o lactantes o cabeza de familia en situación de vulnerabilidad, menores en condición de abandono o protección, etc. |
| **Datos de algún tipo de discapacidad** | Personas con limitaciones sicomotoras, auditivas y visuales, etc. |
| **Datos económicos** | Datos financieros, crediticios y/o derechos de carácter económico de las personas. |
| **Datos socioeconómicos** | Estrato, propiedad de la vivienda, etc. |
| **Datos de información tributaria** | Declaración de impuestos, régimen común o simplificado, etc. |
| **Datos patrimoniales** | Bienes muebles e inmuebles, ingresos, egresos, inversiones, etc. |
| **Datos actividad económica** | Actividad económica NIT |
| **Datos laborales** | Datos relacionados con la historia laboral de la persona, experiencia laboral, cargo, fechas de ingreso y retiro, anotaciones, llamados de atención, etc. |
| **Datos educación** | Datos relacionados con el nivel educativo, capacitación y/o historial académico de la persona, etc. |
| **Datos seguridad social** | EPS, IPS, ARL, fechas de ingreso/retiro EPS, AFP, etc. |
| **Datos de acceso a Sistemas de Información** | Usuarios, IP, claves, perfiles, etc. |
| **Datos gustos y hobbies** | Deportivos, ocio, gastronómicos, turismo, moda, lectura, etc. |
| **Datos Antecedentes** | Datos de antecedentes judiciales y/o disciplinarios |

**DATO PRIVADO**: Es el dato que por su naturaleza íntima o reservada sólo es relevante para el Titular.

**DATO PÚBLICO**: Es el dato calificado como tal según los mandatos de la ley o de la Constitución Política y aquel que no sea semiprivado, privado o sensible. Son públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio, a su calidad de comerciante o de servidor público y aquellos que puedan obtenerse sin reserva alguna. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales, que no estén sometidos a reserva.

**DATOS SENSIBLES**: Son aquellos que afectan la intimidad del Titular de Datos Personales o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos (huella dactilar, el iris del ojo, voz, forma de caminar, palma de la mano o los rasgos del rostro, fotografías, videos, entre otros).

A los Datos Personales de Niños, Niñas y/o Adolescentes, se les aplicarán las mismas normas y procedimientos que a los Datos Sensibles, y no se le dará Tratamiento alguno que pueda vulnerar o amenazar su desarrollo físico, mental y emocional.

**DATOS SEMIPRIVADOS**: Son aquellos que no tienen una naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no solo a su titular, sino a un grupo de personas o a la sociedad en general. Se entiende por dato semiprivado, entre otros, la información relacionada con seguridad social y con el comportamiento financiero y crediticio.

**ENCARGADO DEL TRATAMIENTO**: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de Datos Personales por cuenta del Responsable del Tratamiento.

**GRUPOS DE INTERÉS:** Para los efectos de esta Guía, se entenderán como Grupos de Interés todos los grupos de personas naturales respecto de las cuales el Responsable del Tratamiento y/o los Encargados del Tratamiento realicen algún Tratamiento de Datos Personales.

**INVENTARIO DE BASES DE DATOS:** Documento mediante el cual se identifican las Bases de Datos del Responsable del Tratamiento y se caracterizan de acuerdo al Grupo de Interés, Tipos de Datos y finalidades para el Tratamiento.

**NIÑO O NIÑA:** Personas entre los 0 y 12 años (Código de la Infancia y de la Adolescencia, artículo 3).

**OFICIAL DE PROTECCIÓN DE DATOS PERSONALES:** Persona o Área Responsable de atender las Quejas y Reclamos que se presenten en materia de Protección de Datos Personales, designada en la Política de Privacidad.

**OPERATIVO:** Empleado directo o indirecto del Responsable del Tratamiento que realiza algún tipo de Tratamiento sobre Datos Personales.

**PROTECCIÓN DE DATOS**: Son todas las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

**RESPONSABLE DEL TRATAMIENTO:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la Base de Datos y/o el Tratamiento de los datos.

Para los efectos de esta Guía, se entiende como Responsable del Tratamiento a la Universidad Católica de Manizales.

**TITULAR:** Para los efectos de la Ley 1581 de 2012, es la persona natural cuyos datos personales sean objeto de Tratamiento.

**TRANSFERENCIA:** La Transferencia de datos tiene lugar cuando el Responsable y/o Encargado del Tratamiento de datos personales, ubicado en Colombia, envía la información o los datos personales a un receptor, que a su vez es Responsable del Tratamiento y se encuentra dentro o fuera del país**.**

**TRANSMISIÓN:** Tratamiento de Datos Personales que implica la comunicación de los mismos dentro o fuera del territorio de la República de Colombia cuando tenga por objeto la realización de un Tratamiento por el Encargado por cuenta del Responsable.

**TRATAMIENTO**: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, actualización, uso, circulación, Transferencia, Transmisión o supresión.

## CLASIFICACIÓN DE LAS MEDIDAS DE SEGURIDAD

Las medidas de seguridad se clasifican en tres (3) niveles (Alto, Medio o Bajo), según la Naturaleza del Dato (Público, Semiprivado, Privado, Sensible):

|  |  |
| --- | --- |
| **Naturaleza del Dato** | **Nivel Medida de Seguridad** |
| Público | Bajo |
| Semiprivado | Medio |
| Privado | Medio |
| Sensible | Alto |

Los niveles de seguridad son acumulativos, de forma que las medidas de seguridad para Datos Sensibles incluyen también las medidas de seguridad para los Datos Semiprivados, Datos Privados y Datos Públicos.

## TIPOS DE DATOS Y NIVEL DE SEGURIDAD

|  |  |  |
| --- | --- | --- |
| **Datos Personales** | **Naturaleza del Dato** | **Nivel Medida de Seguridad** |
| Datos de Identificación | Público | Bajo |
| Datos de contacto empresariales o profesionales | Público | Bajo |
| Datos actividad económica | Público | Bajo |
| Datos específicos de Identificación | Semiprivado | Medio |
| Datos económicos | Semiprivado | Medio |
| Datos de información tributaria | Semiprivado | Medio |
| Datos patrimoniales | Semiprivado | Medio |
| Datos laborales | Semiprivado | Medio |
| Datos educación | Semiprivado | Medio |
| Datos seguridad social | Semiprivado | Medio |
| Datos Antecedentes | Semiprivado | Medio |
| Datos de contacto personales | Privado | Medio |
| Datos órdenes para procedimientos médicos | Privado | Medio |
| Datos socioeconómicos | Privado | Medio |
| Datos de acceso a Sistemas de Información | Privado | Medio |
| Datos gustos y hobbies | Privado | Medio |
| Datos Biométricos | Sensible | Alto |
| Datos Resultados y diagnósticos médicos | Sensible | Alto |
| Datos de Asociación | Sensible | Alto |
| Datos sexualidad | Sensible | Alto |
| Datos de Origen | Sensible | Alto |
| Datos de población vulnerable | Sensible | Alto |
| Datos de algún tipo de discapacidad | Sensible | Alto |
| Datos Niños, Niñas y/o Adolescentes | Sensible | Alto |

Los Datos de contacto empresariales o profesionales son de naturaleza Pública, siempre y cuando se utilicen para los fines propios de la empresa o profesión. Sin embargo, adquieren el carácter de privados, cuando se utilizan para otras finalidades. En ese orden de ideas, si los datos se utilizan para otras finalidades, se deberán adoptar medidas de seguridad de nivel Medio.

## CLASIFICACIÓN BASES DE DATOS

|  |  |
| --- | --- |
| **Tipo de Bases de Datos** | |
| **Física** | **Automatizada** |
| Archivo físico | Digital  Electrónica  Medios magnéticos |

## MEDIDAS DE SEGURIDAD

Las siguientes son las medidas de seguridad que deben aplicarse según los Niveles requeridos por la Naturaleza de los Datos según el Tipo de Base de Datos.

Los niveles de seguridad son acumulativos, de forma que las medidas de seguridad para el Nivel Alto, incluyen también las medidas de seguridad para los Niveles Medio y Bajo.

### NIVEL BAJO

|  |  |  |
| --- | --- | --- |
| **Medida de seguridad** | **Tipo de Bases de Datos** | |
| **Física** | **Automatizada** |
| Elaboración, adopción e implementación de Políticas de Protección de Datos Personales | x | x |
| Designación de un Oficial de Protección de Datos Personales quien se encargue de velar por el cumplimiento de las normas de Protección de Datos Personales por parte de los Operativos y Encargados del Tratamiento | x | x |
| Designación de Responsables por Base de Datos, dentro de la organización | x | x |
| Elaboración, seguimiento y control periódico del Inventario de las Bases de Datos de la organización y clasificación según la Naturaleza de Datos Personales que se Traten | x | x |
| Capacitación a los Operativos y a los Encargados del Tratamiento actuales y nuevos ingresos, en materia de Protección de Datos Personales | x | x |
| Elaboración y suscripción de Contratos de Confidencialidad y Transmisión de Datos Personales con los Encargados del Tratamiento | x | x |
| Elaboración y suscripción de Contratos de Confidencialidad y Transferencia de Datos Personales con otros Responsables del Tratamiento a quienes se Transfieran Datos Personales | x | x |
| Elaboración y suscripción de Contratos de Confidencialidad y Protección de Datos Personales con los Operativos | x | x |
| Elaboración, adopción e implementación de Medidas de Seguridad según la Naturaleza de los Datos Personales que se Traten y el Tipo de Base de Datos | x | x |
| Elaboración, adopción e implementación de procedimientos que garanticen una correcta conservación, localización y consulta de la información | x | x |

### NIVEL MEDIO

|  |  |  |
| --- | --- | --- |
| **Medida de seguridad** | **Tipo de Bases de Datos** | |
| **Física** | **Automatizada** |
| Implementación de medidas que eviten el acceso indebido o no autorizado de datos o la recuperación de los que hayan sido descartados, borrados o destruidos garantizando los derechos de los Titulares | x | x |
| Implementación de formatos de autorización para la recuperación de datos que hayan sido descartados, borrados o destruidos por error | x | x |
| Implementación de controles y restricciones de acceso a los Datos Personales que reposen en Bases de Datos Físicas, tales como llaves, códigos de seguridad, carnés para el ingreso, entre otros, y definición de roles y perfiles según los cargos y funciones asignadas a quienes tengan acceso a la información | x |  |
| Implementación de controles y restricciones de acceso a los Datos Personales que reposen en Bases de Datos Automatizadas, tales como creación de usuarios y contraseñas y definición de roles y perfiles según los cargos y funciones asignadas a quienes tengan acceso a la información |  | x |
| Elaboración de lista de usuarios y accesos autorizados e implementación de mecanismos para evitar el acceso a datos distintos de los autorizados | x | x |
| Asignación de deber de diligencia y custodia de la persona a cargo de documentos durante la revisión o tramitación de los mismos. | x |  |
| Autorización del Responsable del Tratamiento para la salida de documentos o soportes por medio físico o electrónico | x | x |
| Elaboración de una matriz de riesgos y elaboración, adopción e implementación de un protocolo de violaciones y atención de incidentes en materia de protección de datos personales | x | x |
| Identificación personalizada de usuarios y contraseñas alfanuméricas secretas para acceder a los sistemas de información, servidores, carpetas compartidas, etc. |  | x |
| Implementación de medidas de acceso a datos y búsqueda de información a través redes y buscadores seguros | x | x |
| Implementación de auditorías ordinarias internas o externas una vez al año y extraordinarias cuando se realicen modificaciones sustanciales en los sistemas de información, así como la conservación del resultado de las mismas y de la prueba de implementación de los planes de acción correspondientes | x | x |
| Implementación de registros de entrada y salida de documentos y reportes que incluyan como mínimo: fecha, emisor y/o receptor, número de documento, tipo de información, forma de envío, responsable de la recepción o entrega | x | x |
| Implementación de mecanismos que limiten el número de intentos reiterados de accesos |  | x |
| Implementación de medidas para la confidencialidad y acceso no autorizado de terceros en el envío de documentos con contenido semiprivado, privado o sensible (ejemplo: sobre sellado) | x | x |
| Implementación de un sistema de copia o back up de la información | x | x |
| Recolección inmediata de copias en el uso de impresoras, escáneres y otros dispositivos de copia | x |  |
| No reutilizar papel que contenga información personal semiprivada, privada o sensible | x |  |
| Implementación de cultura de bloqueo de equipos de cómputo cuando no se encuentren en uso y creación de contraseñas alfanuméricas secretas para el ingreso a la información contenida en los mismos |  | x |
| Limitación al uso de internet mediante bloqueo de páginas inseguras |  | x |
| Limitación al uso del correo electrónico, estableciendo capacidades máximas para el envío de correos |  | x |
| Limitación a las formas de extracción de información, bloqueando puertos de USB y unidad de CD y/o DVD. |  | x |
| Protección de contraseñas siendo las mismas secretas y de carácter intransferible |  | x |
| Compra e implementación de softwares antivirus, antispyware y firewalls que impidan el acceso no autorizado de terceros y la destrucción de la información |  | x |
| Actualización periódica de parches de seguridad |  | x |
| Utilización y compra de licenciamiento de Software original |  | x |
| Implementación de medidas de seguridad en la descarga de archivos adjuntos, como validación de extensiones del archivo (pdf, doc, .xlsx, png, etc.) |  | x |
| Establecimiento de políticas de protección para el acceso remoto a los sistemas de información |  | x |
| Para la atención de requerimientos realizados por alguna autoridad, validación de norma que faculta a la entidad para realizar el requerimiento y verificación de finalidades y proporcionalidad de las mismas según la naturaleza de los datos requeridos y la facultad contenida en las normas | x | x |
| Formateo de equipos de cómputo antes de darles de baja a los mismos |  | x |
| Copia oculta de los contactos en el envío de correos masivos |  | x |

### 

### NIVEL ALTO

|  |  |  |
| --- | --- | --- |
| **Medida de seguridad** | **Tipo de Bases de Datos** | |
| **Física** | **Automatizada** |
| Adopción de medidas que faciliten el control de cambios de la información contenida en las Bases de Datos |  | x |
| Implementación de sistema de etiquetado confidencial | x | x |
| Implementación de mecanismos de cifrado de datos para desarrollos y mantenimientos de equipos informáticos, software, hardware, etc. |  | x |
| Implementación de control y registro de accesos, que contenga información como: usuario, hora, Base de Datos a la que accede, tipo de acceso, registro al que accede, reportes o copias extraídas. | x | x |

## FUNCIONES DEL OFICIAL DE PROTECCIÓN DE DATOS PERSONALES

El Oficial de Protección de Datos Personales, deberá cumplir con las funciones establecidas por la Superintendencia de Industria y Comercio (en adelante “SIC”), en la *Guía para la Implementación del Principio de Responsabilidad Demostrada (Accountability)*, o el documento que lo sustituya, modifique o revoque, para garantizar la Protección de Datos Personales.

A continuación, se enuncian dichas funciones:

* *Promover la elaboración e implementación de un sistema que permita administrar los riesgos del tratamiento de datos personales*
* *Coordinar la definición e implementación de los controles del Programa de Protección de Datos Personales*
* *Servir de enlace y coordinador con las demás áreas de la organización para asegurar una implementación transversal del Programa de Protección de Datos Personales*
* *Impulsar una cultura de protección de datos dentro de la organización*
* *Mantener un Inventario de Bases de Datos Personales en poder de la organización y clasificarlas según su tipo*
* *Registrar las Bases de Datos de la organización en el Registro Nacional de Bases de Datos y actualizar el reporte atendiendo las instrucciones que sobre el particular emita la SIC en caso de estar obligados a ello*
* *Obtener las declaraciones de conformidad de la SIC cuando sea requerido*
* *Revisar los contenidos de los contratos de transmisiones y transferencias de datos que se suscriban.*
* *Analizar las responsabilidades de cada cargo de la organización, para diseñar un programa de entrenamiento en protección de datos personales específico para cada uno de ellos*
* *Realizar un entrenamiento general en protección de datos personales, que tengan acceso por las condiciones de su empleo, a datos personales gestionados por la organización.*
* *Integrar las políticas de protección de datos dentro de las actividades de las demás áreas de la organización*
* *Medir la participación, y calificar el desempeño, en los entrenamientos de protección de datos*
* *Requerir que dentro de los análisis de desempeño de los empleados, se encuentre haber completado satisfactoriamente el entrenamiento sobre protección de datos personales*
* *Velar por la implementación de planes de auditoría interna para verificar el cumplimiento de sus políticas de tratamiento de la información personal*
* *Acompañar y asistir a la organización en la atención de las visitas y los requerimientos que realice la SIC*
* *Realizar seguimiento al Programa de Protección de Datos Personales.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Elaboró** | **Revisó** | **Aprobó** | **Fecha de vigencia** |
| Secretaría General  Asesoría Jurídica | Aseguramiento de la Calidad | Consejo de Rectoría | Junio del 2019 |

**CONTROL DE CAMBIOS**

|  |  |
| --- | --- |
| **ITEM** | **MODIFICACIÓN** |
|  |  |