**TABLA DE CONTENIDO**

| MACROPROCESO | NIVEL 1 | NIVEL 2 |
|---|---|---|
| Gobierno y Gestión | Gestión de Gobierno | Tratamiento de Datos Personales de la Universidad De Los Andes |

## 1. OBJETIVO

Gestionar los incidentes de seguridad asociados a las bases de datos con información personal de la Universidad de Los Andes.

## 2. ALCANCE

El proceso comprende desde la presunción de la ocurrencia de un incidente de seguridad asociado a las bases de datos con información personal, hasta la confirmación del mismo y el reporte del incidente ante la SIC.

## 3. NORMATIVIDAD

- Constitución Política de Colombia, artículos 15 y 20.
- Ley 1266 de 2008.
- Ley 1581 de 2012.
- Decreto 1377 de 2013.
- Decreto Único 1074 de 2015.
- Decreto 090 de 2018.
- Sentencias de la Corte Constitucional C – 1011 de 2008, y C – 748 del 2011.
- Circular 003 de 2018, emitida por la Superintendencia de Industria y Comercio.
- Guías y cartillas emitidas por la Superintendencia de Industria y Comercio.
- Manual de política de tratamiento de datos personales de la Universidad de los Andes.
- Directriz Institucional de seguridad y privacidad de la información de la Universidad de los Andes.

## 4. DEFINICIONES

**Base de datos**: conjunto de datos personales que sea objeto de tratamiento.
**Dato personal**: cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.
**Dato público:** es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.
**Datos sensibles**: se entiende por datos sensibles aquellos que afectan la intimidad del Titular 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.
**Dato privado**: son aquellos que pertenecen única y exclusivamente a la persona sobre la cual recae la información.
**Dato semiprivado**: son aquellos que tienen el carácter de privados y solo le interesan al Titular y a un grupo determinado de personas.
**Incidente de seguridad**: Se refiere a la violación de los códigos de seguridad o la pérdida, robo y/o acceso no autorizado de información de una base de datos administrada por el Responsable del Tratamiento o por su Encargado.
**Titular**: persona natural cuyos datos personales sean objeto de tratamiento.
**SIC:** Superintendencia de Industria y Comercio.
**Registro Nacional de Base de Datos- RNBD-:** Es el directorio público de las bases de datos sujetas a Tratamiento que operan en el país.

## 5. DIAGRAMA DE FLUJO Y DESCRIPCIÓN DE ACTIVIDADES.

### 5.1. Diagrama de flujo – Gestión de incidentes de afectaciones de control de las bases de datos reportadas ante la SIC

### 5.2. Descripción de actividades – Gestión de incidentes de afectaciones de control de las bases de datos reportadas ante la SIC

| | |
|---|---|
| ENTRADA | Presunto incidente |
| SOLICITANTE | Hace referencia al Titular consagrado en la normatividad vigente cualquier persona interna o externa que evidencie el incidente. |
| SALIDA | **1.** Confirmación de reporte del incidente ante la SIC.<br>**2.** Plan de acción interno para mitigar el riesgo de ocurrencia del incidente. |
| DUEÑO DEL PROCESO | Auditoria Interna. |

| | ACTIVIDAD | DESCRIPCIÓN | RESPONSABLE | SISTEMA | DOCUMENTOS |
|---|---|---|---|---|---|
| 1 | Recibir incidente de seguridad asociado a bases de datos | Cualquier persona interna o externa que evidencie el incidente de seguridad asociado a bases de datos, puede reportarlo. | Gestor de protección de datos personales o quien conozca del presunto incidente | | |
| 2 | Reportar incidente | La persona deberá reportar el presunto incidente de manera formal a través de un correo | Gestor de protección de datos personales o | Correo electrónico | |

| | | | | | |
|---|---|---|---|---|---|
| | | electrónico a la cuenta habeasdata@uniandes.edu.co<br><br>dentro de los dos (2) días hábiles de tener conocimiento sobre el mismo. | quien conozca del presunto incidente | | |
| 3 | Analizar información | El Oficial de protección de datos analizará dentro de los cinco (5) días hábiles siguientes, o antes, la solicitud para definir si esta se considera un incidente de seguridad o no, para lo cual se apoyará en las unidades que consideré pertinentes. | Oficial de protección de datos | | |
| 4 | Notificar pasos a seguir a quien reportó el incidente | Si no se considera un incidente de seguridad de datos personales, se notifica a la unidad involucrada los pasos a seguir para mitigar la posible ocurrencia del incidente. | Oficial de protección de datos | Correo electrónico | |
| 5 | Validar con Jurídica/DSIT/ Unidad | Si se considera que el presunto incidente de seguridad de datos personales podría materializarse o se ha materializado, se validará con la Dirección Jurídica sobre si el caso debe o no ser reportado ante la SIC. | Oficial de protección de datos | | |
| 6 | Tomar decisión sobre gestión de incidente junto con Jurídica | Una vez validada la información con la Dirección Jurídica, se determinará si se reporta o no a la SIC. | Dirección Jurídica | | |
| 7 | Comunicar decisión a la unidad | Notificar a la unidad sobre la decisión tomada por el comité frente al incidente. se reporta se informará a la unidad del reporte ante la SIC. | Oficial de protección de datos | Correo electrónico | |

| | | | | | |
|---|---|---|---|---|---|
| 8 | Reportar incidente ante la SIC | El Oficial de Protección de datos realizará el reporte en el Registro Nacional de Bases de Datos administrado por la SIC. https://www.sic.gov.co/registro-nacional-de-bases-de-datos | Oficial de protección de datos | RNBD | |
| 9 | Notificar al Comité de Habeas Data | El Oficial de Protección de Datos notificará en las sesiones del Comité de Habeas Data, el informe semestral de los incidentes que se presenten y la gestión realizada. | Oficial de protección de datos | | |

## 6. RIESGOS

| RIESGO | CAUSAS | CONSECUENCIAS | RIESGO INHERENTE | CONTROLES | RESPONSABLES DE LOS CONTROLES |
|---|---|---|---|---|---|
| No reportar en el término establecido por la normatividad vigente, la información en el Registro Nacional de Bases de Datos. | No reportar los incidentes de seguridad, asociados a bases de datos dentro de los quince (15) días hábiles siguientes a su detección en el Registro Nacional de Bases de Datos. | 1. Multas hasta por el equivalente de dos mil (2.000) SMMLV.<br>2.Suspensión de las actividades relacionadas con el Tratamiento hasta por un término de seis (6) meses.<br>3.Cierre temporal de las operaciones relacionadas con el Tratamiento.<br>4.Cierre inmediato y definitivo de la operación que involucre el | Moderado | Cada vez que se presente un presunto incidente de seguridad asociado a las bases de datos personales, deberá ser informado al Oficial de Protección de Datos, con el fin que el mismo junto con las unidades que considere pertinentes defina si esta se considera un incidente de seguridad o no y de esta manera | Oficial de Protección de datos |

| | | | | | |
|---|---|---|---|---|---|
| | | Tratamiento de datos sensibles.<br>5. Pérdidas económicas y daños reputacionales derivados por sanciones impuestas por la SIC. | | proceder con los pasos a seguir para mitigar la posible ocurrencia del incidente o el reporte del mismo en el Registro Nacional de Bases de Datos, en un plazo no mayor a quince (15) días hábiles después de su ocurrencia de acuerdo a lo establecido en la Circular N° 003 de 2018, emitida por la Superintendencia de Industria y Comercio. | |

## 7. CONTROL DE CAMBIOS

| VERSIÓN | ACTUALIZACIÓN | FECHA |
|---|---|---|
| 0 | | |
| | | |

## 8. APROBACIÓN

| | | | |
|---|---|---|---|
| ELABORÓ | Ingrid Paola Angel | Oficial de protección de datos | 06/2020 |
| ELABORÓ | Sergio Alejandro Rodriguez | Analista de Planeación y Evaluación | 06/2020 |
| REVISÓ | Diana Constanza Garzón | Coordinador Gobierno y cumplimiento de TI | 10/2020 |
| REVISÓ | Adrian Gomez | Auditor de Sistemas | 10/2020 |
| REVISÓ | Camilo Revelo | Abogado | 10/2020 |

| MACROPROCESO | NIVEL 1 | NIVEL 2 |
|---|---|---|
| Gobierno y Gestión | Gestión de Gobierno | Tratamiento de Datos Personales de la Universidad De Los Andes |

| | | | |
|---|---|---|---|
| REVISÓ | Henry Rengifo | Jefe Administración Documental | 10/2020 |
| APROBÓ | Jorge Humberto Charry Endara | Auditor | 15/07/2021 |