Pontificia Universidad
JAVERIANA
Colombia

MANUAL DE PROCEDIMIENTOS DE PROTECCIÓN DE DATOS PERSONALES

2019

TABLA DE CONTENIDO

1. OBJETO 3
2. ALCANCE 3
3. MARCO NORMATIVO 3
4. PRINCIPIOS APLICABLES AL TRATAMIENTO DE DATOS 4
5. DISPOSICIONES GENERALES PARA LA OBTENCIÓN DE LA AUTORIZACIÓN 5
5.1 Contenido de los avisos de privacidad 5
5.2 Autorización en Formatos 6
5.2.1 Autorización en Formatos Web 6
5.2.2 Autorización en formatos físicos 6
5.3 Autorización en la toma de imagen (video y fotografías) 7
5.3.1 Autorización para eventos 7
5.3.2 Autorización para actividades particulares 7
6. GOBIERNO EN LA PROTECCIÓN DE DATOS PERSONALES 7
7. PROCEDIMIENTO DE ATENCIÓN DE CONSULTAS Y RECLAMOS 8
8. ACREDITACIÓN DEL PRINCIPIO DE LA RESPONSABILIDAD DEMOSTRADA (“ACCOUNTABILITY”) Y EL RELACIONAMIENTO CON TERCEROS 9
9. INICIATIVAS QUE IMPLICAN EL TRATAMIENTO DE DATOS PERSONALES Y ANÁLISIS DE IMPACTO DE PRIVACIDAD 10
9.1 Trámite de solicitudes de conceptos o análisis de impacto de privacidad 11
10. PROGRAMA DE SENSIBILIZACIÓN Y CAPACITACIÓN 11
11. VERIFICACIÓN DEL CUMPLIMIENTO DE LAS DISPOSICIONES SOBRE DATOS PERSONALES 11

1. OBJETO

El presente manual tiene el propósito de definir los lineamientos para la implementación, monitoreo, sostenimiento y mejora continua del Programa de Protección de Datos Personales de la Pontificia Universidad Javeriana.

2. ALCANCE

La Pontificia Universidad Javeriana, identificada con Nit. 860.013.720-1, con domicilio principal en la ciudad de Bogotá en la dirección Carrera 7 No. 40 - 62 y su Seccional en la ciudad de Cali ubicada en la dirección Calle 18 No 118 - 250, en adelante denominada como "La Universidad", en el rol de responsable o encargada del tratamiento de los datos personales, está comprometida con el adecuado tratamiento de los datos de sus empleados, los estudiantes, los egresados, los clientes, los proveedores y los terceros. Por lo tanto, en el presente documento se articulan los procedimientos y actividades que involucran el tratamiento de los datos personales, los cuales están alineados con las normas y directrices que lo regulan.

3. MARCO NORMATIVO

Con el propósito de dar un adecuado tratamiento a los datos personales, La Universidad ha identificado el siguiente marco normativo que articula las disposiciones de protección de los datos personales, su confidencialidad y los derechos de los titulares:

- Constitución Política de 1991: En su artículo 15 la Constitución establece lo siguiente*: "(…) Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas. En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución (…)".*

- Ley 1266 de 2008: Por la cual se dictan disposiciones generales del habeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la provenientes de terceros países, y se dictan otras disposiciones.

- Ley 1581 de 2012: Por la cual se dictan las disposiciones generales para la protección de datos personales.

- Decreto Único 1074 de 2015: Por medio del cual se expide el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo.

- Circular Externa 005 de 2017 de la Superintendencia de Industria y Comercio: Por la cual se fijan estándares de un nivel adecuado de protección en el país receptor de la información personal.

- Circular Externa 008 de 2017 de la Superintendencia de Industria y Comercio: Por la cual se incluye un país en la lista de aquellos que cuentan con un nivel adecuado de protección de datos personales.

- Guía de la Superintendencia de Industria y Comercio para la implementación del Principio de Responsabilidad Demostrada (Accountability).

- En general, para la aplicación e interpretación del presente manual, cuando fuere procedente, se aplicarán las demás normas que regulen o complementen lo concerniente a la protección de datos personales.

4. PRINCIPIOS APLICABLES AL TRATAMIENTO DE DATOS

La Universidad está comprometida con el adecuado tratamiento de los datos personales, por lo cual, en todas las actividades que tengan manejo de datos personales, se deberá garantizar la aplicación de los siguientes principios, los cuales se encuentran alineados con los establecidos en el artículo 4 de la Ley 1581 de 2012:

- Legalidad: En todo el proceso de tratamiento de los datos personales, desde el momento de su captura, almacenamiento y eliminación, se debe cumplir con las disposiciones normativas, empleando los datos para fines que estén bajo la ley y a las disposiciones reglamentarias que la desarrollen.

- Finalidad: Todos los datos personales que sean capturados en el desarrollo del ejercicio de las funciones educativas y administrativas que tiene la Universidad, deben atender a finalidades específicas de acuerdo con el tratamiento que se le dará al dato. Las finalidades del tratamiento deben ser informadas a los titulares con el propósito que éstos conozcan las actividades que desarrollará la Universidad con los datos personales que está entregando.

- Libertad: La recolección, almacenamiento y tratamiento de los datos personales sólo puede realizarse con la autorización previa y expresa del titular, quien debe ser informado sobre el tratamiento que se les dará a sus datos personales. La divulgación o socialización de los datos personales sin la previa autorización, o sin una disposición legal que lo habilite, está prohibido.

- Veracidad o calidad: La Universidad debe promover que los datos personales que estarán sujetos a tratamiento deben ser veraces, exactos, completos y actualizados, pues de lo contrario pueden llevar a inducir a errores en la ejecución de tratamiento para el cual fueron capturados.

- Transparencia: Cualquier titular de información podrá tener acceso, en cualquier momento, a la información sobre sus datos personales tratados por la Universidad.

- Acceso y circulación restringida: El tratamiento de los datos personales sólo podrá ser realizado por aquellos que el titular haya efectivamente autorizado, o por las personas habilitadas por las disposiciones legales vigentes.

- Seguridad: Toda la información asociada a los datos personales objeto de tratamiento por parte de la Universidad, deberán protegerse bajo estándares de seguridad adecuados, implementando medidas operativas, técnicas y humanas que eviten su pérdida, adulteración o acceso no autorizado.

- Confidencialidad: La Universidad deberá garantizar la reserva de la información y datos personales que no estén bajo la categoría de datos públicos, por lo cual, todas las personas que tengan acceso al tratamiento de los datos personales deberán promover prácticas de manejo de datos que eviten su exposición o suministro a terceros no autorizados.

5. DISPOSICIONES GENERALES PARA LA OBTENCIÓN DE LA AUTORIZACIÓN

Toda captura, recolección, uso y almacenamiento de datos personales que realice la Universidad en el desarrollo de sus actividades, y de aquellas finalidades dispuestas en la Política de Protección de Datos Personales, requiere de los titulares un consentimiento libre, previo, expreso, inequívoco e informado.

Al efecto, la Universidad ha puesto a disposición de los titulares la autorización para el tratamiento de sus datos personales en los diversos escenarios en los cuales realiza la captura del dato, tanto de manera física como digital, a través de coberturas en modelos de autorizaciones o avisos de privacidad en donde se informa al titular sobre la captura de sus datos personales, el tratamiento al cual serán sometidos incluyendo las finalidades, sus derechos, los canales de ejercicio de sus derechos y la información relacionada sobre la Política de Protección de Datos Personales.

En todos los casos la obtención de la autorización se realizará bajo las diferentes modalidades que establece la ley, teniendo en cuenta la naturaleza de cada uno de los canales de captura de la información, y el modo en que la misma es obtenida, es decir, si es a través de un canal escrito, uno verbal o mediante una conducta inequívoca[1].

Es importante tener en consideración que en todos los casos la Universidad debe custodiar las autorizaciones obtenidas para el tratamiento de los datos personales, dado que ésta hace parte de las pruebas exigidas por la Superintendencia de Industria y Comercio. Así las cosas, se deberán guardar los formatos físicos en donde existan autorizaciones, el registro de llamadas o de los formularios web en los cuales se da trazabilidad sobre la aceptación del tratamiento. La retención documental de las autorizaciones estará alineada con las Tablas de Retención Documental de la Universidad de acuerdo con el tipo de documento que las contiene o a las cuales están asociadas.

5.1 Contenido de los avisos de privacidad[2]

De acuerdo con las disposiciones normativas, los avisos de privacidad mediante los cuales se obtiene la autorización de los titulares deben tener los siguientes elementos:

[1] Decreto 1074 de 2015. Artículo 2.2.2.25.2.4. *Modo de obtener la autorización.* "(…) Se entenderá la autorización cumple con requisitos cuando se manifieste (í) por escrito, (ii) de forma oral o (iii) mediante conductas inequívocas del titular que permitan concluir de forma razonable que otorgó la autorización. ningún caso el silencio podrá asimilarse a una conducta inequívoca (…)".
[2] Decreto 1074 de 2015. Artículo 2.2.2.25.3.3. Contenido mínimo del aviso de privacidad.

a) Nombre o razón social y datos de contacto del responsable del tratamiento
b) El Tratamiento al cual serán sometidos los datos y la finalidad del mismo.
c) Los derechos que le asisten al titular.
d) Los mecanismos dispuestos por el responsable para que el titular conozca la política de Tratamiento de la información.
e) En todos los casos, debe informar al Titular cómo acceder o consultar la política de Tratamiento de información

5.2 Autorización en Formatos

Los modelos de autorización de tratamiento de datos personales pueden ser tramitados a través de formatos web o documentos físicos.

5.2.1 Autorización en Formatos Web

Las áreas que, en el ejercicio de sus funciones, o debido a que lleven a cabo iniciativas que impliquen la recolección de datos personales a través de formularios web, deberán tener en cuenta los siguientes aspectos necesarios para su captura:

a) Solicitar sólo aquellos datos personales necesarios conforme con la finalidad del tratamiento.
b) Relacionar en el formato, un aviso de privacidad que incorpore la autorización del tratamiento por parte del titular.
c) El envío de la información a través del formulario, deberá estar condicionado a la previa aceptación de la autorización de tratamiento del dato.
d) Validar que en el aviso de privacidad se encuentren todas las finalidades de tratamiento asociadas a la captura de los datos personales.
e) Validar que la plataforma que soporta el formulario web tenga la capacidad técnica, operativa y de seguridad para almacenar las autorizaciones, y poder tener la trazabilidad en ellas. Preferiblemente se deberá incluir fecha en la que se obtuvo la autorización.

5.2.2 Autorización en formatos físicos

Las áreas que lleven a cabo iniciativas que impliquen la recolección de datos personales a través de formularios físicos, deberán tener en cuenta los siguientes aspectos:

a) Solicitar sólo aquellos datos personales necesarios conforme con la finalidad de la captura.
b) Relacionar en el formato, un aviso de privacidad que incorpore la autorización del tratamiento de los datos.
c) Para que la Universidad pueda realizar el tratamiento de los datos capturados en el formulario, el titular debe dar la autorización. En el evento en que el titular no haya autorizado, deberá ser analizado de manera independiente.
d) Validar que en el aviso de privacidad se encuentren todas las finalidades de tratamiento asociadas a la captura de los datos solicitados.

e) Garantizar la custodia de los formularios con sus respectivas autorizaciones.

5.3 Autorización en la toma de imagen (video y fotografías)

5.3.1 Autorización para eventos

Con el propósito de cumplir con las disposiciones legales para el tratamiento de datos privados como la imagen, la Universidad ha dispuesto de avisos de privacidad en la entrada de los auditorios.

Sin perjuicio de ello, el área promotora del evento deberá velar por el adecuado cumplimiento de las directrices establecidas sobre protección de datos personales, por lo cual, al inicio de cada presentación se deberá incorporar una diapositiva informativa sobre la captura de la imagen y las finalidades de tratamiento.

5.3.2 Autorización para actividades particulares

Dentro de las actividades que realiza la Universidad, están aquellas en las cuales participan terceros de quienes se puede capturar la imagen por video o fotografía. El área a cargo del tratamiento de los datos gestionará la autorización del titular para el uso de su imagen, garantizando su custodia.

Es importante mencionar que la imagen de los empleados y los estudiantes no requieren de una autorización adicional, ya que la Universidad cuenta con la cobertura en los contratos y en el formulario de registro académico, respectivamente.

Por último, en cada caso se deberá realizar el análisis sobre la imagen que custodiará la Universidad, dado que, si la misma tiene implicaciones sobre derechos de autor, se deberá contar adicionalmente con el consentimiento del autor para hacer uso de ella.

5.4 Custodia de la autorización

Cada área de la Universidad que realice un tratamiento activo de datos personales debe garantizar la custodia y almacenamiento de la autorización para el tratamiento de los datos.

Así mismo, se deberán poner a disposición de la Superintendencia de Industria y Comercio o del Oficial de Protección de Datos en el evento en que éstos lo requieran.

6. GOBIERNO EN LA PROTECCIÓN DE DATOS PERSONALES

La Universidad dentro de su programa de protección de datos personales ha estructurado unos roles para el desarrollo, verificación y control del programa el cual está constituido por:

a) Oficial de Protección de Datos Personales: Es la persona encargada de liderar el programa de protección de datos personales en la Universidad a través de: i) la planeación, ejecución y seguimiento de los elementos que hacen parte del programa; ii) asesorar y sensibilizar a los empleados de la Universidad en relación con el programa y las principales obligaciones en su

ejecución y desarrollo; iii) emitir conceptos y dar respuesta a las inquietudes y requerimientos sobre protección de datos personales a nivel interno y externo, así como asesorar sobre los asuntos relacionados con el manejo de información personal; iv) realizar el seguimiento de las normas sobre protección de datos personales y realizar las adecuaciones pertinentes al programa para procurar su cumplimiento; v) hacer seguimiento a la correcta implementación del programa en la Universidad y vi) gestionar y liderar el proceso de actualización de bases de datos ante el Registro Nacional de Bases de Datos y realizar los reportes legales que los entes de control soliciten.

b) Delegados de Protección de Datos Personales: Son las personas encargadas de las bases de datos identificadas y reportadas antes el Registro Nacional de Bases de Datos, quienes tienen el deber de reportar actualizaciones o cambios sustanciales en la información de la base de datos que deba ser reportada ante la Superintendencia de Industria y Comercio. Adicionalmente, están encargadas de informar sobre cambios en el tratamiento de datos personales, o puntos de captura adicionales que requieran coberturas.

c) Comité de Habeas Data: Está encargado de realizar el seguimiento a los principales temas del programa de protección de datos personales en la Universidad. Es el escenario de control en donde se revisan, discuten, validan y aprueban directrices enfocadas a implementar, consolidar y mejorar continuamente las actividades que hacen parte del programa de protección de datos personales.

Está integrado por, el Oficial de Protección de Datos Personales de la Universidad, y por cada uno de los siguientes miembros:

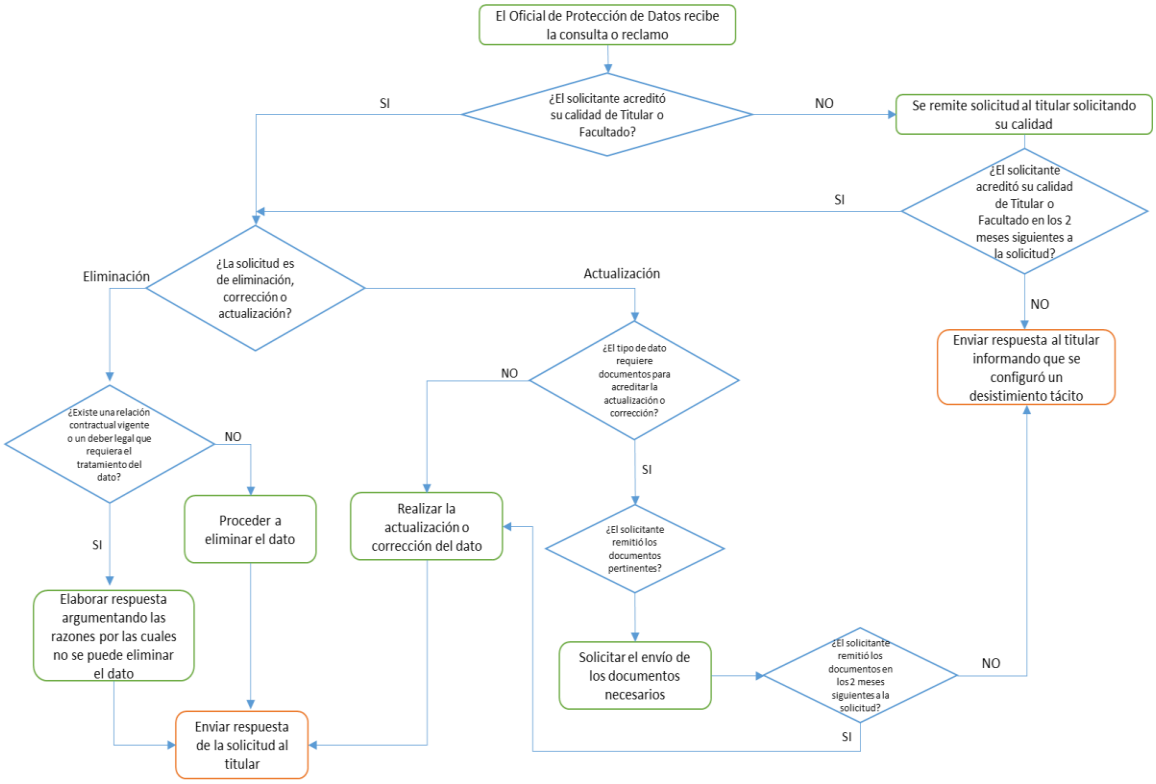
Bogotá	Cali
Secretario General	Secretario General
Director Jurídico	Director Jurídico
Jefe de Seguridad Informática	Coordinadora Seguridad Informática

7. PROCEDIMIENTO DE ATENCIÓN DE CONSULTAS Y RECLAMOS

El procedimiento de consultas y reclamos se ejecutará de acuerdo con los términos incluidos en la ley y acogidos por la Política de Protección de Datos Personales.

Las solicitudes que pueden ser catalogadas como consultas o reclamos pueden llegar por los canales habilitados de protección de datos, los cuales son: usodedatos@javeriana.edu.co y midatopersonal@javerianacali.edu.co, o ser recibidas por cualquier persona vinculada a la Universidad. En éste último caso, es necesario que la solicitud sea remitida al canal de protección de datos personales para que el Oficial de Protección de Datos Personales pueda hacer seguimiento a su trámite y cierre.

A continuación, se presenta el esquema de trámite de consultas y reclamos:



Los tiempos de respuesta de las consultas serán de diez (10) días hábiles desde la fecha de recibo, y de los reclamos serán de quince (15) días hábiles desde su recibo.

En aquellos eventos en los cuales el Oficial de Protección de Datos Personales evidencie que la solicitud del titular no puede ser tramitada debido a que la Universidad debe contar con la información asociada a los datos personales del titular, o porque se encuentra en sistemas de información tecnológicos que requieren de un concepto técnico, podrá integrar una mesa de trabajo entre la Dirección Jurídica, la Dirección de Tecnologías de la Información o el Centro de Servicios y Recursos Tecnológicos, según corresponda, a efectos de contar con un concepto jurídico y técnico integral para dar efectiva respuesta al titular sobre el trámite y cumplimiento de su solicitud.

8. ACREDITACIÓN DEL PRINCIPIO DE LA RESPONSABILIDAD DEMOSTRADA (“ACCOUNTABILITY”) Y EL RELACIONAMIENTO CON TERCEROS

Para llevar a cabo un adecuado tratamiento de los datos personales, el Oficial de Protección de Datos Personales deberá validar los siguientes elementos de manera periódica:

a) Revisión de las actividades que generan algún tipo de tratamiento de los datos personales
b) Validación de los puntos de captura de información personal, identificando el tipo de información que se recolecta y sus finalidades
c) Inventario y actualización de las bases de datos identificadas
d) Seguimiento al cumplimiento de las medidas de seguridad de las bases de datos y repositorios de información que se encuentren en el inventario

e) Identificación de terceros que realizarán el tratamiento de datos personales

Los elementos antes relacionados son la base para la determinación de incorporación de coberturas jurídicas y técnicas en la Universidad, para que se pueda llevar a cabo un adecuado tratamiento de los datos personales en cumplimiento de las disposiciones legales y reglamentarias.

Adicionalmente, como parte de un análisis integral, la Universidad procurará mantener relaciones con terceros que reflejen un compromiso por la protección de los datos personales y la operación que ellos implican. Al efecto, en los contratos que la Universidad suscriba se incorporarán cláusulas de protección de datos personales, y adicionalmente, se podrá solicitar a los terceros en el desarrollo del vínculo comercial o contractual, información que permita validar el cumplimiento de las directrices contenidas en la Política de Protección de Datos Personales de la Universidad, así como aquellas directrices legales y reglamentarias, cuando se estime necesario.

Los terceros que realicen un tratamiento de datos personales de los cuales la Universidad es responsable, deberán acreditar el cumplimiento de los requisitos del régimen de protección de datos personales, aportando: i) la política de protección de datos personales; ii) información sobre los canales habilitados para el trámite de consultas y reclamos y iii) el cumplimiento sobre el registro de las bases de datos ante el Registro Nacional de Bases de Datos de la Superintendencia de Industria y Comercio.

Sin perjuicio de lo anterior, la Universidad podrá realizar verificaciones aleatorias en el desarrollo del vínculo comercial o contractual para validar que se esté efectivamente cumpliendo con las disposiciones de protección de datos, por lo cual se podrá solicitar evidencias o soportes del cumplimiento. En todos los casos, la Universidad podrá incluir cláusulas en los contratos referidas al cumplimiento de las disposiciones sobre protección de datos personales.

En el evento en el cual la Universidad evidencie un incumplimiento de las disposiciones sobre protección de datos por parte del tercero, puede sugerir que se lleve a cabo un acuerdo para su cumplimiento; en el caso en que éste no cumpla, podrá promover la terminación de la relación contractual o comercial vigente.

9. INICIATIVAS QUE IMPLICAN EL TRATAMIENTO DE DATOS PERSONALES Y ANÁLISIS DE IMPACTO DE PRIVACIDAD

La Universidad reconoce la importancia de proteger los datos personales de todos los titulares, es por esto que cualquier tipo de iniciativa que implique el tratamiento de datos personales deberá ser objeto de análisis de manera previa, a efectos de validar el alcance de las coberturas que deben tenerse en cuenta para el desarrollo de la misma.

El análisis de impacto de la privacidad permite validar el cumplimiento de las disposiciones legales y reglamentarias en el ejercicio de la captura y tratamiento de los datos personales en relación con el entorno universitario y los titulares de información.

9.1 Trámite de solicitudes de conceptos o análisis de impacto de privacidad

Los tramites sobre solicitud de conceptos, análisis de impacto de privacidad o coberturas particulares de autorizaciones, serán tramitadas por el Oficial de Protección de Datos Personales a través de la plataforma de Javelex para la sede de Bogotá, y a través de correo electrónico para la sede de Cali.

10. PROGRAMA DE SENSIBILIZACIÓN Y CAPACITACIÓN

Para la Universidad es muy importante tener actualizados a los empleados administrativos y profesores sobre las disposiciones y reglamentación relacionada con la protección de los datos personales.

Al efecto, la Universidad incorporó dentro de su programa de inducción los principales conceptos, lineamientos y disposiciones prácticas sobre el tratamiento de los datos personales, el cual será complementada con la capacitación anual liderada por el área de Gestión Humana.

Adicionalmente, durante cada año se llevarán a cabo capacitaciones por grupos de trabajo que permita comprender y aprehender las directrices sobre manejo de información y medias de seguridad de acuerdo con el desarrollo de la operación de cada área de la Universidad. Los grupos de trabajo que recibirán las capacitaciones serán definidos en la primera sesión del año del Comité de Habeas Data.

11. VERIFICACIÓN DEL CUMPLIMIENTO DE LAS DISPOSICIONES SOBRE DATOS PERSONALES

El Oficial de Protección de Datos Personales podrá, en cualquier momento, adelantar auditorías de supervisión de cumplimiento de las disposiciones sobre protección de datos personales, con el propósito de garantizar el adecuado cumplimiento y desarrollo del programa en la Universidad.

Como resultado de las revisiones pueden levantarse planes de acción para cerrar las brechas encontradas, los cuales tendrán seguimiento en los Comités de Habeas Data.