MANUAL DE PROTECCIÓN DE DATOS

Adaptado a la ley 1581/2012 y decreto 1377 / 2013

Interactuar
Famiempresas que progresan.

CONTENIDO

1. INTRODUCCIÓN 3
2. DEFINICIONES 3
3. OBJETIVO 4
4. OBLIGACIONES DE LOS USUARIOS 4
5. PROHIBICIONES DE LOS USUARIOS 5
6. GESTIÓN DE INCIDENCIAS DE SEGURIDAD 5
7. TRANSFERENCIA DE DATOS PERSONALES 5
8. SOLICITUD DE REQUERIMIENTOS AL OFICIAL DE PRIVACIDAD 6
9. RESPONSABILIDADES DEL OFICIAL DE PRIVACIDAD 7
10. COMITÉ DE PROTECCIÓN DE DATOS 8
11. CLÁUSULAS A INCORPORAR 9
12. AUTORIZACIONES A INCORPORAR 9

1. INTRODUCCIÓN

La protección de los datos de carácter personal de los ciudadanos ha sido regulada por la legislación colombiana mediante la Ley 1581/2012 y el Decreto 1377/2013 que la desarrolla y complementa, y en los cuales se establecen toda una serie de medidas de obligatorio cumplimiento para aquellas entidades que, en el ejercicio de su actividad, sometan a tratamiento este tipo de datos de carácter personal.

El Decreto 1377/2013 tiene como objeto reglamentar parcialmente la Ley 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales.

La Ley de protección de datos y el Decreto 1377, cuyo objeto principal lo constituye la salvaguarda del derecho al honor, la intimidad personal, y la propia imagen de las personas físicas, atribuyen determinadas funciones y obligaciones a todas aquellas personas que intervienen en el tratamiento de las bases de datos donde se almacenan los datos de carácter personal.

La Ley impone sanciones a las organizaciones que no cumplen con dicha reglamentación, que pueden ser de tipo económico o de otro tipo, como suspensión de las actividades, cierre temporal de las operaciones, publicidad de la sanción, inmovilización temporal de la base de datos, etc.

2. DEFINICIONES

2.1 Dato personal
Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.

2.2 Titular
Persona natural cuyos datos personales sean objeto de Tratamiento.

2.3 Tratamiento
Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

2.4 Base de Datos
Conjunto organizado de datos personales que sea objeto de tratamiento.

2.5 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.

2.6 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.

2.7 Usuarios:
Sujeto o proceso autorizado a acceder a datos o recursos.

2.8 Responsable de Seguridad
El responsable del tratamiento designará uno o varios responsables de seguridad encargados de coordinar y controlar las medidas definidas en el documento de seguridad. En ningún caso esta designación supone una delegación de la responsabilidad que corresponde al responsable de la base de datos.

2.9 Autorización
Consentimiento previo, expreso e informado del Titular para llevar acabo el Tratamiento de datos personales.

2.10 Comunicación de datos
Toda revelación de datos realizada a una persona distinta del interesado.

2.11 Requerimiento
Necesidad documentada sobre el uso de bases de datos personales las cuales pueden hacer alusión a: Consultas generales, autorizaciones para transferencia de bases de datos, apoyo en la elaboración de contratos, vistos buenos de Contratos, vistos buenos de envío de información masiva.

2.12 Incidencias de seguridad
Cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos.

3. OBJETIVO

El objetivo de este manual es detallar las funciones y obligaciones que como usuarios de las bases de datos que contienen datos de carácter personal de la Corporación, les corresponde conocer y respetar; así mismo, determinar la participación de los diferentes procesos en la protección de datos de su titular.

4. OBLIGACIONES DE LOS USUARIOS

El personal que para el correcto desarrollo de su labor, tiene autorizado acceso a datos personales, tiene las siguientes obligaciones:

• Guardar el necesario secreto respecto a cualquier tipo de información de carácter personal conocida en función del trabajo desarrollado, incluso una vez concluida la relación laboral con la Corporación.

• Guardar todos los soportes físicos y/o documentos que contengan información con datos de carácter personal en un lugar seguro incluso cuando estos no sean usados, particularmente fuera de la jornada laboral.

• Hacer tratamiento solo de las bases de datos a las cuales está autorizado acceder. Los permisos de acceso de los usuarios son concedidos por el Jefe Directo. En el caso de que cualquier usuario requiera, para el desarrollo de su trabajo acceder a bases de datos o documentos a cuyo acceso no está autorizado, deberá ponerlo en conocimiento del jefe directo

• Comunicar al oficial de privacidad las incidencias de seguridad de las que tenga conocimiento.

• Asegurarse de que no quedan documentos impresos que contengan datos protegidos en la bandeja de salida de la impresora.

5. PROHIBICIONES DE LOS USUARIOS

• Emplear identificadores y contraseñas de otros usuarios para acceder al sistema, tal como lo determina la política D-GTI-01 Políticas de Gestión Tecnológica.

• Burlar las medidas de seguridad establecidas en el sistema informático, intentando acceder a Bases de Datos o programas cuyo acceso no le haya sido permitido.

• Enviar correos masivos empleando la dirección de correo electrónico corporativa.

• El empleo de la red corporativa, sistemas informáticos y cualquier medio puesto al alcance del usuario vulnerando el derecho de terceros, los propios de la organización, o bien para la realización de actos que pudieran ser considerados ilícitos con relación a la protección de datos.

• Copiar la información contenida en las Bases de Datos en las que se almacenen datos de carácter personal a dispositivos personales tales como memorias USB, memorias externas o a cualquier otro soporte sin autorización expresa de su jefe directo.

• Evitar el traslado de cualquier soporte, listado o documento con datos de carácter personal en los que se almacene información fuera de las instalaciones de la Corporación, sin autorización previa del Jefe directo. En el supuesto de existir traslado o distribución de soportes y documentos se realizará cifrando dichos datos, o mediante otro mecanismo que impida el acceso o manipulación de la información por terceros.

6. GESTIÓN DE INCIDENCIAS DE SEGURIDAD

En caso de conocer alguna incidencia de seguridad ocurrida, el usuario debe comunicarla al oficial de privacidad que adoptará las medidas oportunas. Algunos ejemplos de incidencias que pueden afectar a bases de datos son los siguientes:

• Robo o pérdida de llaves de lugares o soportes en donde se almacenen bases de datos.

• Desaparición de documentos o soportes que contengan datos personales.

• Quejas de parte de los clientes que no haya autorizado el uso de sus datos y esté recibiendo llamadas o mensajes de parte de la Corporación.
la impresora.

7. TRANSFERENCIA DE DATOS PERSONALES.

Salida de información: Solo se realizarán salidas de datos personales que estén previamente autorizadas por el oficial de privacidad o que estén amparadas bajo la firma de un contrato o convenio. Las salidas de datos personales de clientes, proveedores, usuarios y empleados deberán hacerse bajos los siguientes lineamientos:

• Deberán adoptarse medidas dirigidas a impedir el acceso o manipulación de la información por parte de terceros.

• Revisar que la finalidad para la cual se va a transferir la base de datos cumpla con las políticas de protección de datos personales.

• Verificar que la base de datos cuente con las autorizaciones de los titulares, para ser compartidas.

• Pedir autorización al jefe del área (Dueño de la información).

• En caso que la transferencia se realice para la ejecución de un proyecto, contrato, acuerdo marco, etc., se debe asegurar que ésta se realice bajos las condiciones pactadas y por medios seguros.

Entrada de información: Cualquier base de datos que ingrese a la Corporación debe estar autorizada por el oficial de privacidad a quién deberán demostrar que la información cuenta con las autorizaciones respectivas para ser tratada. En estos casos la Corporación actuará como encargado de la base de datos y el tratamiento de la información se hará con base en la política de protección de datos (D-EST-03).

8. SOLICITUD DE REQUERIMIENTOS AL OFICIAL DE PRIVACIDAD

Los requerimientos, deben ser remitidos al oficial de privacidad, al correo electrónico protecciondedatos@interactuar.org.co, el cual tiene un plazo máximo de 3 días hábiles para dar respuesta; excepto aquellos casos en los cuales la solicitud se debe escalar al Comité de Privacidad de Datos.

Se recibirán requerimientos para los siguientes conceptos:

Requerimiento	Instrucciones
Consultas generales	Incluir una descripción detallada de la consulta
Autorizaciones para transferencia de bases de datos	1. Incluir el visto bueno del Jefe de área. 2. Detallar la base de datos que se va a transferir: número de registros y campos. 3. Explicar la finalidad de la transferencia. 4. Informar si la base cuenta con la autorización de uso de datos personales y soporte de la misma. 5. Informar si esta transferencia hace parte de la ejecución de un contrato, acuerdo, convenio, etc. de ser así anexar copia del mismo 6. Medio por el cual se va a transferir
Apoyo en la elaboración de contratos en los que se incluye transferencias de bases de datos	Enviar borrador del contrato con una descripción de la solicitud
VoBo de Contratos en los que se incluye transferencias de bases de datos	Diligenciar el F-JUR-01 solicitud de elaboración y revisión de contratos o convenios
VoBo Envío de información masiva	Especificar por qué medio se enviará la comunicación y si la base de datos a la cual está dirigida cuenta con la autorización para uso de datos personales.

Nota:
Si el oficial de privacidad una vez realizado el análisis de la solicitud, considera que necesita el apoyo del Comité de Privacidad, realizará la respectiva consulta o citación a reunión.

9. RESPONSABILIDADES DEL OFICIAL DE PRIVACIDAD

El oficial de privacidad es el encargado de autorizar, coordinar, controlar y en algunos casos ejecutar las medidas de seguridad dispuestas en materia de protección de datos. Cualquier duda o cuestión en materia de protección de datos, debe ser dirigida a dicho oficial.

Las siguientes son las responsabilidades del oficial de privacidad:

- Realizar controles periódicos para verificar el cumplimiento de lo dispuesto en la Política de Protección de datos.
- Validar que toda transferencia de datos personales cumpla con las políticas de protección de datos
- Hacer una correcta gestión de incidencias estableciendo un registro en el que se haga constar el tipo de incidencia, el momento en que se ha producido, o en su caso, los efectos que se hubieran derivado de la misma y las medidas correctivas aplicadas, en relación con las bases de datos.
- Revisar que los datos de carácter personal objeto de tratamiento no se usen para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos.
- Notificar a la Superintendencia la inscripción de nuevas bases de datos.
- Comprobar si se producen transferencias internacionales y si éstas son acordes a Ley 1581 del 2012.
- Mantener un inventario de las bases de datos personales y clasificarlas según su tipo.
- Registrar las bases de datos en el registro nacional de bases de datos y actualizar el reporte atendiendo las instrucciones que sobre el particular emita la SIC
- Atender y dar respuesta a peticiones, quejas o reclamos en materia de protección de datos personales hecha por los titulares de la información.
- Actualizar las políticas de protección de datos, de acuerdo con los cambios presentados en la Corporación, como nuevos negocios, procesos, etc.
- Asegurar que cualquier contrato que se firme integre el clausulado necesario para mitigar jurídicamente los riesgos de fuga de información.
- Recibir requerimientos relacionados con tratamiento de datos y gestionar con el Comité de Protección de Datos los conceptos y recomendaciones de cada integrante, cuando sea requerido.
- Escalar al líder dueño del dato el requerimiento, anexando los conceptos emitidos por el Comité de Protección de Datos
- Administrar la agenda del Comité de Protección de Datos, identificando los temas a tratar en la reunión periódica y convocando reunión extraordinaria, cuando se requiera.
- Emprender campañas de formación y sensibilización para los empleados en materia de protección de datos personales. Estas campañas tendrán como objetivo que los empleados conozcan, acepten y cumplan las políticas de tratamiento de información.

10. COMITÉ DE PROTECCIÓN DE DATOS

Objetivos:

- Asegurar el compromiso de la Corporación con la protección de datos de los grupos de interés.

- Aprobar los cambios realizados a las políticas de protección de datos.

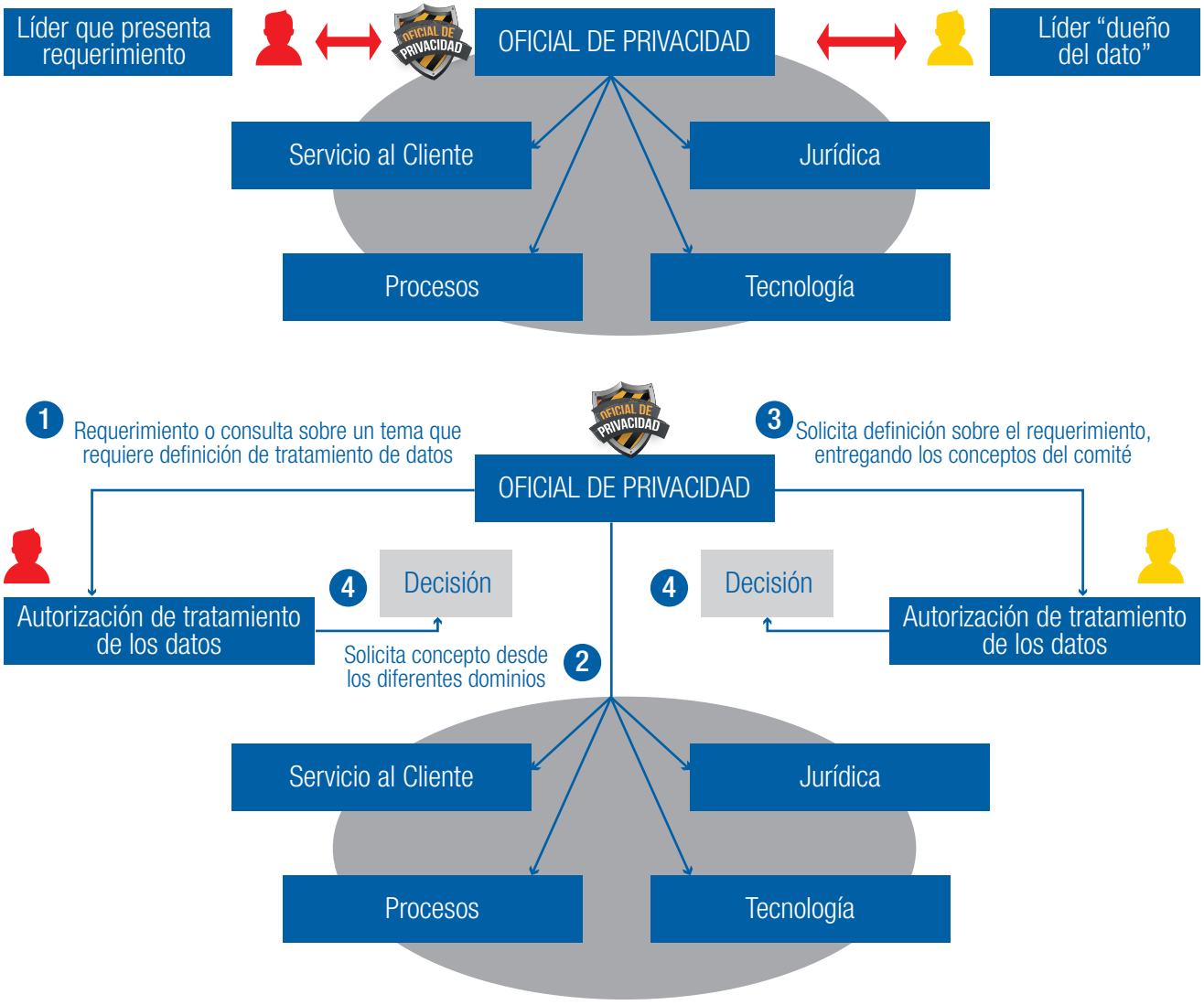
- Asegurar que la organización incorpora en sus procesos, registros, sistemas de información y bases de datos, los mecanismos para asegurar el adecuado tratamiento de los datos.

- Asegurar el cumplimiento de la normatividad de Protección de datos aplicable a los procesos y contratos.

Los integrantes del Comité se pueden consultar en el Anexo 01 Anexo de Comités del proceso Gestión de Comunicaciones.

Modelo de gestión del Comité de Protección de datos

COMITÉ PROTECCIÓN DE DATOS | Modelo de Gestión



Responsabilidades del comité de protección de datos:

• Definir y aprobar los cambios en las políticas de tratamiento de información.

• Analizar cambios organizacionales o requerimientos de las diferentes áreas de la Corporación, que involucren tratamiento de datos y requieran definiciones a nivel contractual, procedimental, tecnológico y de atención al cliente.

• Emitir conceptos desde cada dominio involucrado, sobre requerimientos de las diferentes áreas o entidades.

• Escalar al Comité Directivo temas que represente riesgos o requieran decisiones de alto impacto para la Corporación.

• Asesorar al oficial para que en la Corporación se garanticen, por encima de todo, los derechos fundamentales de intimidad y el adecuado tratamiento de la información de los grupos de interés.

11. CLÁUSULAS A INCORPORAR

Todas las relaciones contractuales que involucran el manejo de información personal requieren de una regulación con la que se obligue al cumplimiento de la Ley 1581 de 2013 como sus Decretos reglamentarios, es por esto que se diseñaron cláusulas que deben ser incluidas en todos los contratos, acuerdos, convenios etc. que involucren transferencia de datos personales; las cuales se pueden consultar en el Anexo 01 Cláusulas, Acuerdos y Autorizaciones Protección de Datos.

12. AUTORIZACIONES A INCORPORAR

La normatividad en materia de protección de datos personales establece que para el tratamiento de información personal, es obligatorio contar con la autorización del titular de esa información, la cual debe ser previa, expresa e informada. Dichas autorizaciones se pueden consultar en el Anexo 01 Cláusulas, Acuerdos y Autorizaciones Protección de Datos.

TALENTO HUMANO

Este proceso es el responsable de velar por la protección de datos del personal contratado ya sea por medio de un contrato laboral o de prestación de servicios; para tal fin, se define incluir dentro de los contratos, cláusulas de confidencialidad laboral, violación de datos personales y daño informático; las cuales pueden ser consultadas en el Anexo 01 Cláusulas, Acuerdos y Autorizaciones Protección de Datos.

GESTION DE COMPRAS

Como proceso responsable de la contratación y compra de productos y servicios, debe velar porque se respete la confidencialidad como contratante y contratista, por lo tanto se incluye en los contratos con terceros que involucren datos personales (transferencia, transmisión, cesión, venta, etc.), un contrato de transmisión de datos personales.

GESTION COMERCIAL DE SDE

Se encarga de realizar las ventas de los servicios de desarrollo empresarial, y dentro de la protección de datos, tiene un rol muy importante, ya que en éste, se debe solicitar la autorización por parte de los clientes para el manejo de datos sensibles; así mismo, en los casos en que los menores de edad adquieran uno de los servicios, obtener la debida autorización por parte de su padre o tutor. Ver Anexo 01 Cláusulas, Acuerdos y Autorizaciones Protección de Datos.

Interactuar
Famiempresas que progresan.

Corporación Interactuar @Interactuar @CorpInteractuar

www.interactuar.org.co