MANUAL DE PROTECCIÓN DE DATOS

Interactuar
Famiempresas que progresan.

Manual de Protección de Datos

CONTENIDO

Manual de Protección de Datos

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 la cual se establecen una serie de medidas de obligatorio cumplimiento para aquellas entidades que, en el ejercicio de su actividad, sometan a tratamiento[1] este tipo de datos de carácter personal.[2]

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 dentro del país o cuando el responsable o encargado de la información no está establecido en el territorio nacional, le sea aplicable la legislación colombiana en virtud de normas y tratados internacionales.

Dicha Ley de protección de datos y su Decreto reglamentario, cuyo objeto principal lo constituye la salvaguarda del derecho al buen nombre, la intimidad personal, y la propia imagen de las personas[3], atribuye determinadas responsabilidades y obligaciones a todas aquellas personas que intervienen en el tratamiento de las bases de datos donde se recolectan, usan o almacenan los datos de carácter personal.

La Ley establece sanciones para las organizaciones y responsables que no cumplan con dicha reglamentación, que pueden ser de tipo económico o de otra naturaleza, tales como suspensión de las actividades, cierre temporal de las operaciones, publicidad de la sanción, suspensión temporal de la facultad de hacer tratamiento de datos personales e incluso el cierre definitivo de operaciones.

2. DEFINICIONES

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

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

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

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

---

[1] Dicha Ley 1581 de 2012 define en el numeral g del artículo 2° el tratamiento como "cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión"
[2] La Ley 1581 de 2012 define en el numeral c del artículo 2° el dato personal como "Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables"
[3] El fundamento constitucional para la expedición de la legislación de protección de datos es el artículo 15 de la constitución política que establece: "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".

Manual de Protección de Datos

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 personales.

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.

Usuarios:
Colaborador, aliado, contratista o proceso autorizado a acceder y/o tratar los datos o recursos bajo responsabilidad de la Corporación

Administrador de tratamiento de base de datos:
El responsable del tratamiento designará uno o varias áreas administradoras en el tratamiento bases de datos personales encargadas de gobernar, manejar y velar por el cumplimiento de las medidas, procedimientos y directrices definidas en la política de tratamiento de datos personales, el manual de seguridad de la información y las políticas internas definidas por el responsable sobre los datos personales de los cuales son administradoras. En ningún caso esta designación supone una delegación de la responsabilidad que corresponde al Responsable de la base de datos.

Autorización:
Consentimiento previo, expreso e informado del Titular para llevar a cabo el tratamiento de datos personales.

Comunicación, transferencia o trasmisiones:
Toda revelación autorizada de datos realizada a una persona distinta del titular.

Requerimiento de datos personales:
Necesidad justificada de un colaborador a área administradora sobre el uso de datos personales o bases de datos personales de clientes, colaboradores, proveedores o cualquier grupo de interés. Dicha necesidad puede hacer alusión a: consultas generales en el ejercicio de las actividades propias de la Corporación, autorizaciones para transferencia o trasmisión de bases de datos, apoyo en la elaboración, modificación o revisión de contratos, vistos buenos y autorizaciones para el envío o acceso de información masiva relacionada con datos personales.

Incidentes de seguridad de la información:
Cualquier anomalía o situación que pueden ocurrir en el procesamiento de los datos e información de la Corporación y que afecten o pudiera afectar a la seguridad sobre los activos de información -incluyendo datos personales- a nivel de confidencialidad, integridad y disponibilidad de los datos.

Oficial de Privacidad:
Persona o área encargada por el Responsable del tratamiento que busca velar, coordinar, preservar y encaminar la implementación efectiva de las políticas y procedimientos adoptados por el responsable para el cumplimiento de la ley, y la aplicación de buenas prácticas de gestión de datos personales dentro de la Corporación.

Manual de Protección de Datos

3. OBJETIVOS

El objetivo de este manual de protección de datos es describir actividades y lineamientos que se relacionan con las políticas y procedimientos relacionados con el tratamiento de datos personales en Interactuar.

Para lograrlo, se busca la implementación de procesos organizados y sistemáticos en el tratamiento de datos personales que permita a Interactuar:

- Dar a conocer de manera detallada a los usuarios de las bases de datos que contienen datos de carácter personal de la Corporación los deberes y responsabilidades que les corresponde conocer y cumplir.
- Precisar la participación de los diferentes procesos o áreas de la Corporación en la protección de datos personales de clientes, colaboradores, proveedores o cualquier grupo de interés.
- Enmarcar y definir las actividades a cargo del Oficial de la Privacidad en ejercicio de su rol.
- Contribuir con la implementación de medidas dentro de la entidad que permitan cumplir con los principios y finalidades de la legislación colombiana relacionada con datos personales.

4. OBLIGACIONES DE LOS USUARIOS

El colaborador, aliado, contratista o área/proceso autorizado que, para el correcto desarrollo de su labor, tiene acceso o hace tratamiento a datos personales además de los deberes establecidos en la ley y la política de tratamiento de datos personales fijada por INTERACTUAR, tendrá las siguientes obligaciones:

- Cumplir con los principios aplicables al tratamiento de datos personales contenidos en la Ley 1581 de 2012; en especial, seguridad, confidencialidad, acceso y circulación restringida, finalidad, deber de información, legalidad, entre otros.
- 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, comercial o contractual con la Corporación. En especial la información de carácter privado o sensible según la Ley 1581 de 2012.
- Guardar todos los soportes y/o documentos físicos o digitales que contengan información con datos de carácter personal en un lugar seguro, con medidas de seguridad si es el caso, incluso cuando estos no sean usados, particularmente fuera de la jornada laboral con el fin de garantizar las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
- Hacer tratamiento (almacenar, usas, modificar, consultar, compartir, eliminar) solo a los datos personales o las bases de datos a las cuales está autorizado, en las condiciones de dicha autorización. Los permisos de acceso de los usuarios son concedidos por el área de Infraestructura Tecnológica con el VoBo de Talento y Desarrollo Organización, o quien haga sus veces, su líder inmediato y las demás áreas que se consideren pertinentes en cada caso. En el evento de que cualquier usuario requiera justificadamente, para el desarrollo de su trabajo acceder, usar o hacer tratamiento a bases de datos o documentos a cuyo acceso no está autorizado o que sobrepasen sus atribuciones, deberá ponerlo en conocimiento de su líder inmediato y solicitar las autorizaciones y accesos pertinentes.
- Velar por la confidencialidad de las bases de datos por lo que los datos personales los compartirá única y exclusivamente a los colaboradores que tengan necesidad de conocerla en desarrollo

- de sus funciones, a quienes se les advertirá sobre el carácter especial de la información y las medidas de protección pertinentes, para así evitar que se divulgue, revele o publique sin autorización.
- En caso de tener conocimiento sobre incidentes de seguridad dar inicio al procedimiento de gestión de incidentes establecido (P-GSI-02) por la Corporación, teniendo en cuenta lo indicado en el numeral 7° de este manual.
- Asegurarse de que no quedan copias, impresiones o accesos que contengan datos protegidos que puedan permitir la consulta o acceso no autorizado por terceros, por ejemplo, documentación en la bandeja de salida de la impresora.
- Velar y garantizar el carácter facultativo de la obtención de datos cuando estas versen sobre datos personales de carácter sensibles.
- Utilizar las herramientas de copia oculta del correo electrónico para realizar él envió de correos electrónicos a direcciones electrónicas que no son corporativas.

5. PROHIBICIONES DE LOS USUARIOS

- No es permitido emplear identificadores, usuarios y contraseñas de otros usuarios o colaboradores para acceder al sistema, tal como lo determina la política D-GTI-01 Políticas de Gestión Tecnológica. Tampoco es permitido compartir el identificador, usuario o contraseña asignada por la Corporación con otros usuarios o colaboradores.
- Burlas o evadir las medidas de seguridad establecidas en los sistemas informáticos de la Corporación, intentando acceder a bases de datos, información o programas cuyo acceso no le haya sido permitido o sea controlado.
- 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 para la realización de actos que pudieran ser considerados ilícitos con relación a la protección de datos personales, vulnerando el derecho de terceros o los propios de la organización
- Copiar la información contenida en las Bases de Datos en las que se almacenen datos de carácter personal de clientes, colaboradores y proveedores a dispositivos personales tales como memorias USB, memorias externas, alojamiento de archivos en la nube o a cualquier otro soporte, sin autorización previa y expresa de su líder inmediato, quien determinará la pertinencia de dicha acción. En el supuesto de existir comunicación, traslado, transferencia o trasmisión de bases de datos se implementarán medias de seguridad adicionales idóneas como establecimiento de contraseñas o procesos de cifrando y enmascaramiento[4] o cualquier otra forma que impida el acceso o manipulación de la información por terceros no autorizados.
- El traslado de cualquier soporte, listado o documento físico en los que se almacene información con datos de carácter personal fuera de las instalaciones de la Corporación sin autorización previa y expresa de su líder inmediato, quien determinará la pertinencia de dicha acción. En el supuesto de existir comunicación, traslado, transferencia o trasmisión de soportes y documentos se implementarán medias de seguridad adicionales idóneas para impedir el acceso o manipulación de la información por terceros no autorizados.

[4] El cifrado, enmascaramiento o anonimización de datos hace referencia a procesos informáticos de tratamiento de los datos personales que impiden la identificación de una persona de manera directa o indirecta.

Manual de Protección de Datos

6. TRATAMIENTO DE DATOS SENSIBLES

La Corporación Interactuar, teniendo en cuenta su Política de tratamiento de datos personales publicada en su página web, en especial lo indicado en su numeral 9°, 9.1 y 12 podrá solicitar datos personales relativos a la salud de los trabajadores, clientes, contratistas y visitantes, siempre de manera voluntaria y con el cumplimiento de los requisitos para la recolección de datos sensibles establecido en la Ley 1581 de 2012. Dicha información al ser considerado como un dato sensible, requiere un manejo especial que incluye además de los requisitos generales de la autorización para la recolección de cualquier tipo de dato personal, medidas de recolección, almacenamiento y uso especiales:

Dicho tratamiento será en todos los casos antecedido por la autorización expresa e informada de los titulares de los datos y sus finalidades serán las ya establecidas por las políticas de tratamiento de datos de la Corporación y por los deberes legales fijados por la legislación colombiana respecto a la identificación y mitigación de cualquier riesgo biológico, físico o químico, y la implementación de acciones que garanticen la protección integral de los trabajadores, clientes, contratistas y demás personas que estén presentes en las Instalaciones de Interactuar.

a. Condiciones de recolección

El manejo de estos datos relativos a la salud son datos sensibles y su suministro es de carácter facultativo y no obligatorio por parte de los trabajadores y usuarios de la Corporación. El tratamiento de estos datos se realizará para las finalidades antes establecidas y para la mitigación del riesgo biológico generado por el COVID-19 y será autorizado de manera expresa y previa por el titular, de acuerdo con lo que indica la ley.
La declaración del estado de salud se hace bajo juramento del titular de que toda la información proporcionada es verídica, y autoriza que la Corporación pueda verificar dicha información, y en caso de inexactitud pueda aplicar las sanciones o las medidas establecidas por la ley y las políticas internas.

b. Condiciones de almacenamiento.

La Corporación Interactuar utiliza diferentes medidas técnicas y procedimientos de seguridad de la información tendientes a garantizar la integridad, disponibilidad y confidencialidad de los datos personales sensibles suministrados. Así mismo evita su adulteración, perdida, consulta, uso, acceso, o divulgación no autorizada o fraudulenta. Para ello cuenta con los siguientes controles:

- Seguridad de acceso: La información de acceso no será proporcionada, ni trasferida, trasmitida o vendida a terceros, ni reutilizada con otros fines diferentes a los mencionados anteriormente
- Recopilación de la información: La Corporación solicita datos sensibles a través de plataformas seguras, y son almacenados en la infraestructura interna dispuesta para ello, de manera segura.
- Acceso controlado a la red y dispositivos autorizados: El acceso a la red se restringe solo a los usuarios autorizados para acceder a los datos que sean estrictamente necesarios, con la directriz de que dicho acceso se realice a través de dispositivos propios de la Corporación o autorizados.

c. Condiciones de uso y circulación

Esta información, será utilizada únicamente por la Corporación Interactuar con las finalidades antes mencionada, en donde por regla general en caso de que sea maneja por personal externo se utilizarán técnicas y herramientas para anonimizar los datos y que estos no estén asociados o vinculados a una persona en particular. Solo en casos de requerimientos debidamente formulados por las autoridades sanitarias, se podrá circular a estos esta información, en donde se preferirá remitir los datos estrictamente necesarios y anonimizados, de tal forma que no se pueda identificar el titular del dato. Solo excepcionalmente se tratará la información de forma no anónima cuando es rigurosamente necesario conocer la identidad del titular del dato y conforme a lo dispuesto en la Ley 1581 de 2012 y sus decretos reglamentarios.

d. Condiciones de eliminación

En caso de que el titular solicite la supresión total o parcial de los datos sensibles -la revocatoria de la autorización- la Corporación se abstendrá de hacer uso de los mismo, y comunicará al titular el estado de la revocatoria. Sin embargo, no procederá la eliminación de los datos en el caso de que el titular tenga algún deber legal o contractual de permanecer en la base de datos administrada por la Corporación.

Las consultas y reclamaciones presentadas se tramitarán de acuerdo con los procesos y procedimientos internos, a través de los canales de contacto dispuestos por la Corporación. Tratándose de excolaboradores o usuarios inactivos, la Corporación almacenará, aun después de finalizado el contrato de trabajo o vinculo contractual o legal, la información necesaria para cumplir con las obligaciones que puedan derivarse en virtud de la relación laboral, contractual o extracontractual que existió conforme a la legislación colombiana.

7. PERIODOS DE CONSERVACIÓN DE DATOS PERSONALES

En concordancia con el principio de finalidad contenido en la Ley 1581 de 2012, la conservación de los datos personales recolectados y tratados por Interactuar corresponderán a que verdaderamente exista una finalidad clara para realizar el tratamiento de dichos datos. Su periodo de conservación se encuentra incluido en las tablas de retención establecidas entre la gestión documental y cada área responsable de bases de datos.

8. GESTIÓN DE INCIDENTES DE SEGURIDAD

Si bien es cierto que la Corporación como responsable o encargado tiene el deber de adoptar las medidas necesarias para evitar posibles afectaciones a la seguridad de los datos, es necesario contemplar la posibilidad de que dichas medidas de seguridad fallen, y que sea necesario mitigar los riesgos y daños que se pueden causar a los derechos y libertades fundamentales de los Titulares y a las organizaciones.

Las afectaciones más comunes a los datos personales son de tres categorías:

I. Confidencialidad: Casos en los que, por la acción de un hacker u otra conducta criminal o por efecto de un error de un colaborador, uno o varios archivos con datos personales llega a manos de terceras personas no autorizadas.

Manual de Protección de Datos

II. Integridad: El dato personal es alterado total o parcialmente, y se pierde su trazabilidad y confiabilidad.
III. Disponibilidad: El acceso a un dato o a un conjunto de datos personales queda restringido para que personas autorizadas accedan, lo que afecta el ejercicio del objeto de Interactuar.

Algunos ejemplos de situaciones relacionadas con datos personales que pueden conllevar posibles incidentes de seguridad son los siguientes:

- Robo o pérdida de llaves de lugares o soportes físicos y virtuales en donde se almacenen bases de datos personales.
- Desaparición de documentos o soportes que contengan datos personales.
- Peticiones, quejas o reclamos masivos hecho por titulares sobre una misma irregularidad sobre el tratamiento de sus datos personales.
- Fuga o acceso no autorizado a sistemas que contengas información o bases de datos personales.

En caso de tener conocimiento o sospechas soportadas de la ocurrencia de algún posible incidente de seguridad ocurrido, el usuario debe comunicarlo al correo electrónico seguridad@interactuar.org.co o al canal asignado por la Corporación para dar inicio al procedimiento de gestión de incidentes establecido (P-GSI-02).

A su vez y de acuerdo con la gestión de incidentes, este primer punto de contacto definido por la entidad informará al Oficial de Privacidad al correo electrónico protecciónde datos@interactuar.org.co cuando dicho incidente esté o pueda estar relacionado con datos personales para adoptar las medidas preventivas, reactiva y correctivas legales y oportunas para la mitigación del daño a los titulares del presunto incidente.

Una vez comunicado el hecho y se haya hecho la evaluación preliminar y buscado implementar las medidas técnicas para la contención del incidente de seguridad por partes del primer punto de contacto; el Oficial de privacidad en colaboración con las áreas correspondientes deberá propender por:

- Una adecuada evaluación de riegos e impactos asociados al incidente.
- La identificación de posibles daños para las personas, empresas o sociedad en general.
- El reportar a la Superintendencia de Industria y Comercio la ocurrencia del incidente de seguridad[5] dentro del término establecido por la ley6. Esta notificación debe contener como mínimo la información que establece el Registro Nacional de Bases de Datos (RNBD).
- El análisis de necesidad, pertinencia y eventual modalidad de comunicar a los titulares la ocurrencia del incidente.
- La gestión estrategias para prevenir futuros eventos que puedan afectar los datos personales que han tratado.

[5] Literales n) y k) de los artículos 17 y 18 de la Ley 1581 de 2012

Manual de Protección de Datos

9. TRANSFERENCIA O TRANSMISIÓN DE DATOS PERSONALES.

La salida de información de datos personales sea por transferencia o transmisión, deberá en todos los casos estar previamente autorizada por el Oficial de Privacidad o estar amparadas bajo la firma de un contrato, alianza o convenio. Las salidas de datos personales de clientes, proveedores, usuarios, colaboradores o cualquier grupo de interés deberán hacerse bajos los siguientes lineamientos:

- Revisar que la finalidad para la cual se va a transferir la base de datos cumpla con las políticas de protección de datos personales.
- Remitir la información relacionada con datos personales estrictamente necesaria para la realización de la relación contractual, comercial que soporta la necesidad de la transferencia o transmisión.
- Verificar que la base de datos cuente con las autorizaciones de los titulares, para ser compartidas.
- Pedir autorización a las áreas administradoras de la información.
- En caso de 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.
- En caso de tratarse de trasmisiones de datos personales a terceros, recordar a ese tercero:
  - El carácter de información confidencial de esta información.
  - El deber de que esas BBDD estén almacenadas en lugares seguros y con acceso restringido a las personas que directamente están implicadas en las tareas acordadas.
  - La calidad de encargado que poseen, es decir, esas BBDD deben ser manejadas siempre acorde a los parámetros de la Corporación respecto a tratamiento de datos por lo que cualquier manejo diferente a las actividades por las cuales se compartió la información o cualquier inconveniente con los datos debe ser comunicado y autorizado por la Corporación.
- Adoptarse medidas de seguridad dirigidas a impedir el acceso o manipulación de la información por parte de terceros no autorizados. Dichas medidas dependerán dl nivel de riesgo, cantidad y tipo de datos personales a compartir e incluyen:
  - Con ayuda del área de Tecnología de Información o Riesgos, cifrar, enmascarar o anonimizar la información relacionada con datos personales, tales como: nombres, datos comerciales, datos financieros, datos de contacto -teléfonos y direcciones-, entre otros.
  - Tener en cuenta que si hay varios archivos que tienen dicha información confidencial, las reglas de enmascaramiento deben ser las mismas en todos los archivos, para poder hacer los cruces respectivos.
  - Enviar los datos en Excel o en .zip, pero protegidos por una clave segura para apertura (más de 8 posiciones, que combinen mayúsculas, minúsculas, números y caracteres especiales).
  - Enviar la clave por otro medio diferente al que se envían los datos, y si es posible segmentada en diferentes medios.
  - En caso de requerir enviar continuamente información que contenga datos personales validar la pertinencia de definir canales más seguros (tales como FTPs, sFTP o similares).

Manual de Protección de Datos

En el caso de tratarse de base de datos que ingresen a la Corporación, estas deben estar previamente autorizadas por el Oficial de Privacidad o estar amparadas bajo la firma de un contrato, alianza o convenio, a quién deberán evidenciar que la información cuenta con las autorizaciones respectivas para ser tratada. En estos casos debe quedar expresamente acordado con la otra parte si la Corporación si se comparte en calidad de transferencia o transmisión para determinar las facultades y deberes de Interactuar en el tratamiento de datos.

10. SOLICITUD DE REQUERIMIENTOS AL OFICIAL DE PRIVACIDAD

Los requerimientos, deben ser remitidos al oficial de privacidad, al correo electrónico protecciondedatos@interactuar.org.co, quien contará con los tiempos de entrega y ANS establecidos en el procedimiento gestión requerimientos asesora jurídica P-JUR-01; excepto si te trata de casos en los cuales la solicitud se debe escalar o consultar al Comité de Seguridad de la Información, en donde se dará respuesta lo más pronto posible.

Se recibirán requerimientos relacionados con el tratamiento de datos personales para los siguientes conceptos:

Tipo de requerimiento	Documento para adjuntar	Entregables
Consultas generales/ Revisión de documentos legales.	-Descripción detallada de la consulta. -Documento que se va a revisar y anexos pertinentes.	Correo del visto bueno de parte del Oficial de Privacidad con documentos ajustados o comentados.
Autorizaciones para transferencia o trasmisión de bases de datos, sean masivas o no.	-Detallar la base de datos que se va a transferir: número de registros y campos (no incluir la BBDD) -Explicar la finalidad de la transferencia. -Incluir vistos buenos de áreas administradoras de los datos -Informar si la base cuenta con la autorización de uso de datos personales. -Medio y medidas de seguridad para realizar la transferencia o transmisión -Informar si esta transferencia o transmisión hace parte de la ejecución de un contrato, acuerdo o convenio, de ser así anexar copia del mismo.	Correo del visto bueno de parte del Oficial de Privacidad o solicitud de ampliación o complementación de solicitud.

Elaboración, modificación o revisión de contratos, convenios o acuerdos en los que se incluye transferencia o transmisión de bases de datos.	- Diligenciar el F-JUR-01 solicitud de elaboración y revisión de contratos o convenios -Enviar borrador del contrato y anexos pertinentes cuando aplique. Nota: Tener en cuenta que de acuerdo con la Política de Compras cuando se trate de contratos es necesario que la elaboración, revisión o modificación provenga directamente del área de Compras.	Correo del visto bueno de parte del Oficial de Privacidad con borrador de contrato, convenio o acuerdo ajustado o comentado.
Conceptos Jurídicos	-Descripción detallada de la consulta -Documento y anexos pertinentes si aplica.	Concepto elaborado

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

11. RESPONSABILIDADES DEL OFICIAL DE PRIVACIDAD

Como prevé la legislación, todo responsable y encargado debe designar a una persona o área que "asuma la función de protección de datos personales que dará trámite a las solicitudes

de los Titulares, para el ejercicio de los derechos a que se refiere la Ley 1581 de 2012 (...)"[7]

El oficial de privacidad es el encargado dentro de la Corporación de velar por la implementación efectiva de las política y procedimientos adoptados para el cumplimiento de las normas. Cualquier duda o cuestión en materia de protección de datos, debe ser dirigida a dicho oficial.

- Las siguientes son las responsabilidades y actividades que debe realizar el oficial de privacidad:
- Autorizar, coordinar y apoyar activamente en la ejecución de la implementación de medidas de seguridad dispuestas en materia de protección de datos.
- Realizar controles periódicos para verificar el cumplimiento de lo dispuesto en la Política de Protección de datos.
- Validar que las transferencia y transmisiones de datos personales cumplan con las políticas de protección de datos.
- Hacer una correcta gestión de incidentes relacionados con datos personales de acuerdo con lo estableciendo en este manual y en el procedimiento de gestión de incidentes establecido (P-GSI-02).

[7] De acuerdo con lo indicado en el artículo 23 del decreto 1377 de 2013

- 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.
- Realizar la inscripción y actualización de nuevas bases de datos o de cambios sustanciales en el Registro Nacional de Bases de datos administrado por la Superintendencia de Industria y Comercio.
- Comprobar si se producen transferencias o transmisiones internacionales y si éstas son acordes a Ley 1581 del 2012.
- Mantener un inventario de las bases de datos personales manejadas por la Corporación.
- Notificar a la Superintendencia de Industria y Comercio a través de los canales habilitados los incidentes de seguridad relacionados con datos personales.
- 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.
- Verificar que cualquier contrato, convenio o acuerdo que se firme y que se relacione con el tratamiento de datos personales integre el clausulado necesario para mitigar jurídicamente los riesgos de fuga de información, de acuerdo con anexo 01.
- Recibir y gestionar los requerimientos realizados y hacer las consultas al Comité de Seguridad de la Información sobre sus conceptos y recomendaciones, cuando sea requerido.
- Según corresponda, escalar al solicitante, el usuario y el administrador de la base de datos los conceptos y decisiones emitidos por el Comité de Seguridad de la Información.
- Asistir y participar activamente en las reuniones periódicas del Comité de Seguridad de la Información, fomentando la inclusión en el orden del día los temas identificados sobre datos personales a tratar y solicitar reuniones extraordinarias con algunas o todas las áreas que conforman el comité cuando se requiera.
- Emprender junto a las áreas idóneas campañas de formación, comunicación y sensibilización para los colaboradores en materia de protección de datos personales. Estas campañas tendrán como objetivo crear una cultura de protección de datos done los colaboradores conozcan, acepten y cumplan las políticas de tratamiento de datos personales establecidas.

12. REGISTRO Y ACTUALIZACIONES PERIODICAS DE BASE DE DATOS

De acuerdo con lo indicado por el Decreto 090 de 2018 del Ministerio de Comercio, Industria y Turismo, modificado por la Circular 003 de 2018 expedida por la SIC las personas jurídicas de naturaleza pública y las sociedades y entidades sin ánimo de lucro con activos totales superiores a 100.000 UVT ($3.630.800.000 para 2021) deben inscribir en el Registro Nacional de Bases de Datos-RNBD información sobre sus bases de datos físicas o digitales que contengan datos personales.

Como responsable del tratamiento de datos personales, Interactuar deben cumplir las siguientes obligaciones respecto al RNBD:

- La actualización contenida en el RNBD se realizará anualmente entre el 2 de enero y el 31 de marzo.

- Se deben reportar al RNBD los incidentes de seguridad (perdida, robo y/o acceso no autorizado) dentro de los quince (15) días hábiles siguientes al momento en que se detecte o sea puesto en conocimiento del Oficial de Privacidad.
- Cuando se genere una nueva base de datos por parte del Responsable del tratamiento, la misma deberá registrarse dentro de los dos meses siguientes a su creación.
- Cuando se realicen cambios sustanciales[8] en la información reportada en el RNBD, esta deberá actualizarse dentro de los primeros 10 días hábiles de cada mes.

Los cambios sustanciales que ocurran en las bases de datos utilizadas por la Corporación deben ser comunicadas por las áreas administradoras de la base de datos al Oficial de Privacidad con la finalidad de que este último pueda cumplir su deber de actualización. Dicha notificación debe ser comunicada a través del correo electrónico protecciondedatos@interactuar.org.co con la siguiente información:

- Detallar la base de datos a crear o que va a tener el cambio sustancial: número de registros y campos (no incluir la BBDD)
- Explicar la razón de generación de la nueva base de datos o del cambio sustancial, indicando cuál es el cambio sustancial.
- Incluir vistos buenos de áreas administradoras de la base de datos a crear o que tendrá cambios sustanciales.

13. INFORMES A LA ALTA DIRECCIÓN SOBRE GESTIÓN DE TRATAMIENTO DE DATOS

Se remitirá de manera anual, durante el primer semestre del año inmediatamente siguiente, un informe sobre la Gestión de tratamiento de datos personales a la Alta Dirección de la Corporación, con el fin de que la misma se encuentre informada de las acciones, requerimientos, hallazgos y resultados relacionados con el tratamiento de datos personales realizado por Interactuar.

Estos informes permitirán que la Alta Dirección pueda tomar decisiones estratégicas para el desarrollo de un sistema de gestión de datos personales dentro de la Corporación.

La elaboración de dichos informes estará a cargo del Oficial de Privacidad, quien con el apoyo de las áreas administradoras de datos realizará y validará la información contenida. Dichos informes se presentarán con los indicadores establecidos para dicha gestión y contendrán a su vez información cualitativa y cuantitativa sobre los avances en el desarrollo de la gestión en tratamiento de datos.

[8] Son cambios sustanciales los que se relacionen con la finalidad de la base de datos, el encargado de tratamiento, los canales de atención al titular, la clasificación o tipo de datos almacenados en cada base de datos, las medidas de seguridad de la información implementada, la política de tratamiento de la información y la transferencia o transmisión internacional de datos personales.

Manual de Protección de Datos

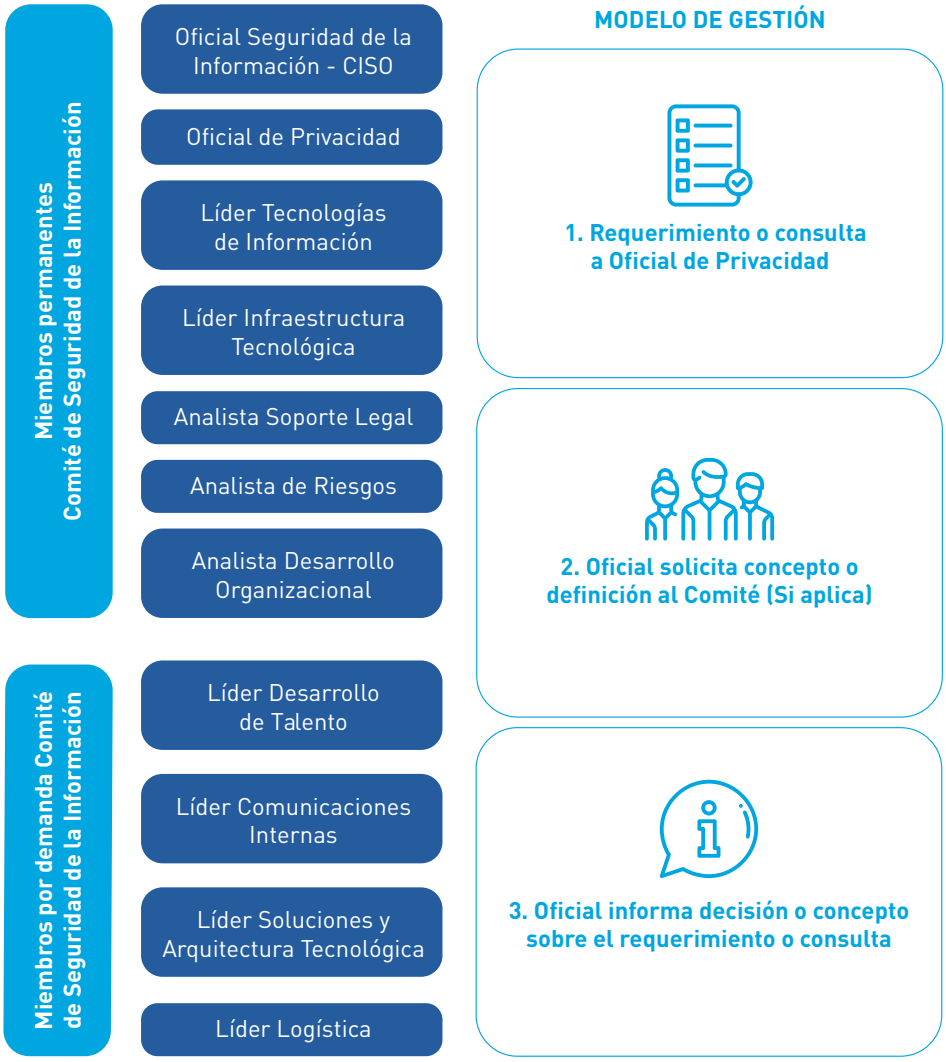
14. PARTICIPACIÓN EN COMITÉ DE SEGURIDAD DE LA INFORMACIÓN (GSI)

Teniendo en cuenta que la protección de los datos personales y sus políticas y lineamientos deben estar en todo momento alineados con la seguridad de la información de Interactuar y que son dos componentes que propenden por proteger los pilares de la confidencialidad, la integridad y la disponibilidad de la información (que incluye los datos personales) se toma la determinación de que el órgano de discusión y decisión sobre la estrategia general relacionada con datos personales dentro de la Corporación será el Comité de Seguridad de la Información, en donde actuará como miembro permanente el Oficial de Privacidad.

Dentro de los objetivos de este comité relacionados con datos personales esta:

- 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 Listado Comités del proceso Administración de Gobierno Corporativo (A-GGC-03).



Manual de Protección de Datos

Dentro de las responsabilidades del Comité de Seguridad de la Información respecto a la protección de datos se encuentran:

- Definir y aprobar los cambios en las políticas de tratamiento de datos.
- Analizar cambios organizacionales o requerimientos de las diferentes áreas de la Corporación, que involucren tratamiento de datos y requieran definiciones a nivel estratégico, contractual, procedimental, y/o tecnológico.
- Emitir conceptos o lineamientos desde cada área miembro sobre requerimientos o consulta sobre tratamiento de datos de las diferentes áreas.
- Escalar al Comité Directivo temas que represente riesgos o requieran decisiones de alto impacto para la Corporación.
- Asesorar al Oficial de Privacidad para que en la Corporación se garanticen, por encima de todo, los derechos fundamentales al buen nombre, la intimidad personal, la propia imagen de las personas y el adecuado tratamiento de la información de los grupos de interés.

15. MEDICIÓN Y MEJORA CONTINUA EN LA GESTIÓN DE TRATAMIENTO DE DATOS

Buscando la maduración y mejora continua en los procesos relacionados con la gestión de datos personales de la Corporación se establecen las siguientes medidas:

- La medición del impacto de las gestiones realizadas por la Corporación para la implementación de un sistema de gestión de datos personales a través del (los) indicador(es) de gestión definido(s) en la matriz de indicadores F-MAI-02.
- Teniendo en cuenta los procesos de calidad usados por la Corporación, se implementarán, cuando sea pertinente, el registro de acciones correctivas, preventivas y de mejora (ACPM) en las herramientas establecidas desde la gestión de datos personales.
  Esto con el propósito de registrar las oportunidades de mejora y eficiencias y realizar junto a Desarrollo Organizacional el calculo de madurez de procesos, teniendo en cuenta el nivel de madurez de la gestión de datos personales, el procedimiento de mejora continua P-GDO-04 y el anexo niveles madurez procesos A-GDO-16 establecidos.

16. CLÁUSULAS PARA 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 por lo que se diseñaron cláusulas que deben ser incluidas en los contratos, acuerdos, convenios o alianzas que involucren transferencia o transmisión de datos personales; las cuales se pueden consultar en el Anexo 01 Cláusulas, Acuerdos y Autorizaciones Protección de Datos (A-GGC-06).

17. AUTORIZACIONES PARA INCORPORAR

La normatividad en materia de protección de datos personales establece que, por regla general 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 Anexo 01 Cláusulas, Acuerdos y Autorizaciones Protección de Datos (A-GGC-06).

Manual de Protección de Datos

18. ÁREAS O GESTIONES ADMINISTRADORAS DE TRATAMIENTO DE BASES DE DATOS

a. Talento humano

Este proceso es el responsable de velar por la protección de datos de los colaboradores contratados ya sea por medio de un contrato laboral o de prestación de servicios; para tal fin, se define incluir dentro de los contratos, cláusula de violación de datos personales y daño informático; cláusula de protección, consulta y tratamiento de datos personales; las autorizaciones generales que se requieran; las cuales pueden ser consultadas en el Anexo 01 Cláusulas, Acuerdos y Autorizaciones Protección de Datos.

b. Gestión de compras

Como proceso responsable de la contratación y compra de productos y servicios, debe velar porque se respete el tratamiento de datos personales respecto a proveedores sean contratantes o contratista, por lo tanto, se incluye en los contratos con terceros que involucren datos personales (transferencia, transmisión, cesión, venta, etc.) cláusulas y autorizaciones tales como cláusula de confidencialidad general; cláusula de acciones civiles y penales; cláusula de devolución o destrucción de la información; cláusula tratamiento de datos personales en calidad de encargado; cláusula de notificación de incidentes de seguridad relacionado con datos personales; Autorización manejo de datos personales proveedores, clausula para trasmisión o transferencia de datos personales.

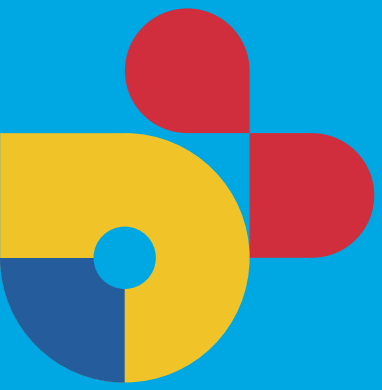
c. Gestión comercial

Se encarga de ejecutar la estrategia del CORE del negocio (financiero), a través de un equipo comercial que genera valor a los prospectos y empresarios; 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 y prospectos para el tratamiento de datos personales. De acuerdo con el Anexo 01 Cláusulas, Acuerdos y Autorizaciones Protección de Datos dicha gestión debe incluir autorización manejo de datos personales clientes; Autorización manejo de datos personales clientes.

19. CARÁCTER VINCULANTE Y SANCIONES

Las disposiciones y directrices contenidas en el presente documento vinculan a todos los colaboradores de la Corporación por lo que dar cumplimiento a este es un deber de todos los trabajadores.

Su incumplimiento u omisión pueden conllevar que se incurra en una falta y al establecimiento de la sanción disciplinaria correspondiente o incluso a una eventual terminación del contrato de trabajo, de acuerdo con lo indicado en los capítulos XIII y XIV del Reglamento Interno de Trabajo de la Corporación.



CORPORACIÓN INTERACTUAR

@CORPINTERACTUAR

CORPORACIÓN INTERACTUAR

CORPORACIÓN INTERACTUAR

Interactuar

Famiempresas que progresan.