

	<b>MANUAL DE PRIVACIDAD, PROTECCIÓN Y TRATAMIENTO DE DATOS PERSONALES</b>	Código:GYD-MA-008
		Versión:001
		Vigencia:2023-01-06

## ORGANIZACIÓN CLÍNICA BONNADONA PREVENIR

### MANUAL DE PRIVACIDAD, PROTECCIÓN Y TRATAMIENTO DE DATOS PERSONALES

Elaboró	Última Actualización Realizada Por:	Última Revisión Realizada Por:	Aprobó
<b>Juan Manuel Castilla</b> Asistente Jurídico	N.A	<b>Fabian Pinedo</b> Director de sistema	<b>Dr. Carlos Osorio</b> Gerente

#### INTRODUCCION

La ORGANIZACIÓN CLÍNICA BONNADONA PREVENIR S.A.S (OCBP) identificada con NIT 800.194.798-2, informa los pacientes, usuarios, personal en proceso de selección, colaboradores, proveedores, clientes corporativos y accionistas (TITULARES) que se compromete a proteger y conservar la información de Datos Personales bajo las condiciones de seguridad necesarias, tendientes a evitar el uso no autorizado, fraudulento, así como la adulteración o pérdida de la información de Datos Personales, con el fin de propender por el respeto de éstos.

Para los efectos, la OCBP coloca a disposición de los actuales y futuros TITULARES de Datos Personales, contenidos o que se lleguen a contener en nuestras Bases de Datos, el siguiente MANUAL DE POLITICAS DE PRIVACIDAD, PROTECCIÓN Y TRATAMIENTO DE DATOS PERSONALES DE LA ORGANIZACIÓN CLÍNICA BONNADONA PREVENIR S.A.S, el cual se compone de los siguientes contenidos:

1. OBJETIVO
2. JUSTIFICACIÓN

3. ALCANCE
4. DEFINICIÓN DE TÉRMINOS
5. LINEAMIENTOS
6. LEGISLACIÓN APLICABLE
7. DESARROLLO PRIMARIO
  - 7.1 PRINCIPIOS PARA EL TRATAMIENTO DE DATOS PERSONALES
  - 7.2 RESPONSABLE DEL TRATAMIENTO Y AMBITO DE APLICACIÓN
  - 7.3 AUTORIZACIONES
  - 7.4 MANEJO DE DATOS PERSONALES Y SENSIBLES CON PROVEEDORES.
8. DERECHOS Y DEBERES DEL TITULAR
  - 8.1 DEBERES DE LA ORGANIZACIÓN CLINICA BONNADONA PREVENIR COMO RESPONSABLE DE LOS DATOS PERSONALES
9. TIPO DE INFORMACION REGISTRADA
10. CLASIFICACIÓN DE BASES DE DATOS EN LA ORGANIZACIÓN CLÍNICA BONNADONA PREVENIR S.A.S Y FINALIDAD.
11. SEGURIDAD DE LA INFORMACIÓN
12. TRANSFERENCIA Y TRANSMISIÓN DE DATOS PERSONALES
13. GOBIERNO EN LA PROTECCIÓN DE DATOS PERSONALES
14. PROCEDIMIENTO POR PQRS Y ACTUALIZACIÓN DE DATOS SENSIBLES
15. PROCEDIMIENTO DE MANEJO DE DATOS SIN AVISO DE PRIVACIDAD
16. SENSIBILIZACIÓN Y CAPACITACIÓN
17. MODIFICACIONES Y VIGENCIA
18. EVALUACIÓN Y SEGUIMIENTO.

## **1. OBJETIVO**

Establecer un marco integral y actualizado para la gestión, protección y tratamiento de datos personales en conformidad con las regulaciones legales vigentes, garantizando la confidencialidad, integridad y disponibilidad de la información, así como fomentando la concientización y capacitación constante de todo el personal involucrado en el manejo de datos dentro de la empresa.

Así mismo desarrollar un manual exhaustivo de privacidad y tratamiento de datos personales que garantice la seguridad, confidencialidad y cumplimiento normativo en el manejo de la información de pacientes de la OCBP, colaboradores y proveedores. De igual forma, implementar programas de capacitación continua para todo el personal, asegurando un manejo adecuado y ético de datos sensibles, fortaleciendo la conciencia y responsabilidad en la gestión de la información.

## **2. JUSTIFICACIÓN**

La OCBP desarrolla este manual, en estricto cumplimiento de la Ley Estatutaria 1581 de 2012 y su decreto reglamentario 1377 de 2013. Con la implementación de este manual se asegura la confidencialidad y debido manejo de la información que se obtenga, registre, use, transmita y actualice mediante autorización previa, expresa y voluntaria del TITULAR de la información.

La OCBP garantiza a todos los TITULARES que hayan facilitado o lo hagan en el futuro, la custodia y privacidad de sus Datos Personales. En especial, sensibles obtenidos a través de los pacientes, los cuales se encuentran contenidos en las Historias Clínicas, la cual está regulada por la Ley 23 de 1981 y la Resolución 1995 de 1999, y la OCBP se ciñe a sus parámetros, con el fin de cumplir con los protocolos de diligenciamiento, administración, conservación, custodia y confidencialidad que se requieren por la normatividad señalada, por el Ministerio de Salud y el Archivo General de la Nación.

## **3. ALCANCE**

La política de privacidad, protección y tratamiento de Datos Personales, se aplica a los Datos de los TITULARES, que sean personas naturales, y de la cual La OCBP ostenta información, en las bases de Datos, sean éstas físicas o digitales.

A la vez, este documento propende por ser un instrumento con el que los TITULARES puedan ejercer el derecho fundamental al habeas data, el cual les permite ejercer sus derechos de conocer, actualizar y ratificar los datos que se encuentren en nuestras bases de datos.

#### 4. DEFINICIONES

- DATO PERSONAL: Es cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables, como el nombre, la edad, el sexo, el estado civil, el domicilio, entre otros.
  - DATO PRIVADO: Es el dato que por su naturaleza íntima o reservada sólo es relevante para el TITULAR.
  - DATO SEMIPRIVADO: Es semiprivado el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su TITULAR sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio de actividad comercial o de servicios a que se refiere el Título IV de la Ley 1266.
  - DATO PÚBLICO: Es el dato calificado como tal según los mandatos de la Ley o de la Constitución Política y todos aquellos que no sean semiprivados o privados”, de conformidad con la Ley 1266 de 2008. “Son públicos, entre otros, los Datos contenidos en documentos públicos, sentencias judiciales debidamente ejecutoriadas que no estén sometidos a reserva y los relativos al estado civil de las personas.
  - DATOS SENSIBLES: Son 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.
- 
- La Ley 1581 de 2012, prohíbe el tratamiento de Datos sensibles con excepción de los siguientes casos:
    - Cuando el TITULAR otorga su consentimiento
    - El Tratamiento es necesario para salvaguardar el interés vital del TITULAR y éste se encuentre física o jurídicamente incapacitado
    - El tratamiento es efectuado en el curso de las actividades legítimas y con las debidas garantías por parte de una fundación, ONG, asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que se refieran exclusivamente a sus miembros o a las personas que mantengan contactos regulares por razón de su finalidad
    - El Tratamiento se refiera a Datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial,
    - El Tratamiento tenga una finalidad histórica, estadística o científica, en este último caso deben adoptarse las medidas conducentes a la supresión de identidad de los TITULARES.
- 
- DATOS PERSONALES DE LOS NIÑOS, NIÑAS Y ADOLESCENTES: Se debe tener en cuenta que aunque la Ley 1581 de 2012 prohíbe el tratamiento de los Datos Personales de los niños, niñas y adolescentes, salvo aquellos que por su naturaleza son públicos, la Corte Constitucional precisó que independientemente de la naturaleza del dato, se puede realizar el tratamiento de éstos *“siempre y cuando el fin que se persiga con dicho tratamiento responda al interés superior de los niños, niñas y adolescentes y se asegure sin excepción alguna el respeto a sus derechos prevalentes”*.
  - AUTORIZACIÓN: Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales
  - AVISO DE PRIVACIDAD: Es la comunicación verbal o escrita generada por el Responsable, dirigida al Titular para el Tratamiento de sus Datos Personales, mediante la cual se le informa acerca de la existencia de las políticas de Tratamiento de información que le serán aplicables, la forma de acceder a las mismas y las finalidades del Tratamiento que se pretende dar a los Datos Personales.
  - ENCARGADO: Es la persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de Datos Personales por cuenta y encargo del Responsable.
  - AUTORIZADO: Es la Compañía y todas las personas bajo la responsabilidad de la Compañía que por virtud de la Autorización y de esta Política, tienen legitimidad para Tratar los Datos Personales del Titular. El Autorizado incluye al género de los Habilitados.
  - CONTRATO DE PROTECCIÓN DE DATOS: Es la legitimación que expresamente y por escrito mediante contrato o documento que haga sus veces, otorgue la Compañía a terceros, en cumplimiento de la Ley aplicable, para el Tratamiento de Datos Personales, convirtiendo a tales terceros en Encargados del Tratamiento entregados o puestos a disposición.
  - CONSULTA: Solicitud del titular del dato o las personas autorizadas por éste o por la ley para conocer la información que reposa sobre ella en bases de datos o archivos.
  - Manual: Es el Manual Interno de Políticas y Procedimientos para la Protección de Datos Personales de la Compañía, en el cual están consignados las políticas y procedimientos para garantizar el adecuado cumplimiento de la Ley.
  - RESPONSABLE: El Responsable del Tratamiento de los datos personales es una 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 mismos.
  - TITULAR: Es la persona natural o jurídica a quien se refiere la información que reposa en una Base de Datos y quien es el sujeto del derecho de hábeas data, por ser titular de los Datos Personales correspondientes.
  - TRANSFERENCIA: envía la información o los datos personales a un receptor, que a su vez es Responsable del Tratamiento y se encuentra dentro o fuera del país.
  - TRANSMISIÓN: Es la comunicación de los datos personales, dentro o fuera del territorio de la República de Colombia y tiene por objeto la realización de un tratamiento por el Encargado por cuenta del Responsable.
  - TRATAMIENTO: Es toda operación o conjunto de operaciones, electrónicas o no, que permitan la recolección, conservación, ordenamiento, almacenamiento, modificación, relacionamiento, uso, circulación, evaluación, bloqueo, destrucción y, en general, el procesamiento de Datos Personales, así como también su transferencia a terceros a través de comunicaciones, consultas, interconexiones, cesiones, mensajes de datos.
  - SARLAFT: El Sistema de Administración del Riesgo de Lavado de Activos y de la Financiación del Terrorismo, se compone de dos fases: la primera corresponde a la prevención del riesgo y cuyo objetivo es prevenir que se introduzcan al sistema financiero recursos provenientes de actividades relacionadas con el lavado de activos y/o de la financiación del terrorismo. La segunda, que corresponde al control y cuyo propósito consiste en detectar y reportar las operaciones que se pretendan realizar o se hayan realizado, para intentar dar apariencia de legalidad a operaciones vinculadas al LA/FT. Ver circular Externa de Superfinanciera 026 de 2008.

## 5. LINEAMIENTOS

A continuación, se establecen los lineamientos generales aplicados por la OCBP con el fin de cumplir con sus obligaciones en cumplimiento de los principios para la administración de datos personales. Estos lineamientos son complementarios a las políticas, procedimientos o instructivos generales actualmente existentes e implementados y en ningún momento pretenden reemplazarlas o desconocerlas, por lo que en la OCBP debe tenerse en cuenta para el presente Manual los siguientes parámetros:

**a. Captura de información:** Si la captura se hace en un medio físico, la autorización cuenta con la firma del titular de los datos; si se utiliza un medio tecnológico o verbal, se implementan mecanismos eficientes que permitan la conservación de su aceptación al tratamiento de los datos por parte de la entidad. En los casos en que la OCBP actúe como responsables de las bases de datos y sin importar el medio de captura, se obtiene autorización del Titular de la información y se guarda prueba de la misma, a menos que dicha autorización se haya otorgado por parte del titular por medio de acciones inequívocas, tales como aceptar comunicaciones por parte de la entidad y responderlas.

La ley 1581 de 2012 artículo 10 establece: La autorización del Titular no será necesaria cuando se trate de: a) Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial; b) Datos de naturaleza pública; c) Casos de urgencia médica o sanitaria; d) Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos; e) Datos relacionados con el Registro Civil de las Personas.

Para acceder a los Datos Personales deberá en todo caso cumplir con las disposiciones contenidas en la ley mencionada anteriormente.

**b. Autorización:** De conformidad con las normas vigentes, el consentimiento del Titular de los datos debe cumplir con las siguientes características: 1. Ser previo: Debe otorgarse antes de la incorporación del dato a la base de datos. 2. Ser expreso: Otorgarse de forma inequívoca, explícita y concreta para la finalidad que requiere. 3. Ser informado: El Titular del dato debe conocer la finalidad de la base de datos y el tratamiento que se le va a dar a sus datos; así como ser consciente de los efectos de su autorización. En concreto, es obligatorio informar al titular de los datos: (i) El tratamiento que se hará sobre sus datos y la finalidad del mismo; (ii) el carácter facultativo de las respuestas a las preguntas que versen sobre datos sensibles; (iii) los derechos que tiene; (iv) la identificación, dirección física o electrónica del responsable del tratamiento. Para obtener la autorización se siguen las siguientes instrucciones: En primer lugar, antes de que la persona autorice se le informará de forma clara y expresa lo siguiente: • El tratamiento al cual serán sometidos sus datos personales y la finalidad del mismo. • El carácter facultativo de la respuesta a las preguntas que le sean hechas, cuando estas hacen referencia expresa sobre datos sensibles o sobre los datos de niñas, niños o adolescentes. • Los derechos que le asisten como titular previstos en el artículo 8 de la ley 1581 de 2012. En segundo lugar, obtiene el consentimiento del titular a través de cualquier medio que pueda ser objeto de consulta posterior. Los mecanismos podrán ser predeterminados a través de medios técnicos que faciliten al titular su manifestación automatizada. Se entiende, como se indicó anteriormente, que la autorización cumple con estos requisitos cuando se manifiesta por: 1. Escrito: Se deja prueba del cumplimiento de la obligación de informar y del consentimiento. Si el titular solicita copia, deberá suministrársele. 2. Verbalmente: A través de llamadas telefónicas en las cuales el titular es informado de sus derechos y las finalidades de tratamiento de la información dándole la oportunidad a continuación de manifestar su aceptación. De dichas comunicaciones, y si se cuenta con los medios, se dejará prueba a través de grabaciones conservadas de manera que puedan ser objeto de posterior consulta. 3. Conductas inequívocas del titular: La autorización también puede obtenerse a partir de conductas inequívocas del Titular del Dato que permitan concluir de manera razonable que éste otorgó su consentimiento para el tratamiento de su información. En ningún caso, el silencio del Titular podrá considerarse como una conducta inequívoca.

**c. Autorización para tratamiento de datos sensibles:** La OCBP solo puede realizar operaciones o tratamientos de los datos sensibles con autorización expresa del titular de dichos datos personales, siempre y cuando se haya informado al titular: Cuando se trate de la recolección de datos sensibles se deben cumplir los siguientes requisitos: • La autorización debe ser explícita. • Se debe informar al Titular que no está obligado a autorizar el tratamiento de dicha información. • Se debe informar de forma explícita y previa al Titular cuáles de los datos que serán objeto de tratamiento son sensibles y la finalidad su uso.

**d. Autorización de tratamiento de datos de niños, niñas o adolescentes (NNA):** Cuando se trate de la recolección y tratamiento de datos de niños, niñas o adolescentes se deben cumplir los siguientes requisitos: • La autorización debe ser otorgada por personas que estén facultadas para representar los NNA. El representante de los NNA deberá garantizarles el derecho a ser escuchados y valorar su opinión del tratamiento teniendo en cuenta la madurez, autonomía y capacidad de los NNA para entender el asunto. • Se debe informar que es facultativo responder preguntas sobre datos de los NNA. • El tratamiento debe respetar el interés superior de los NNA y asegurar el respeto de sus derechos fundamentales.

**e. Prueba de la autorización:** Con el fin de que posteriormente se pueda consultar la autorización, la OCBP conservará prueba de esta. En cuanto a las autorizaciones en Formatos Web se deberán tener en cuenta los siguientes aspectos necesarios para su captura: Solicitar sólo aquellos datos personales necesarios conforme con la finalidad del tratamiento. Relacionar en el formato, un aviso de privacidad que incorpore la autorización del tratamiento por parte del titular. El envío de la información a través del formulario deberá estar condicionado a la previa aceptación de la autorización de tratamiento del dato. Validar que en el aviso de privacidad se encuentren todas las finalidades de tratamiento asociadas a la captura de los datos personales. 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.

Ahora bien, en lo que respecta a las Autorizaciones en formatos físicos: Las unidades que lleven a cabo iniciativas que impliquen la recolección de datos personales a través de formularios físicos, deberán tener en cuenta los siguientes aspectos: Solicitar sólo aquellos datos personales necesarios conforme con la finalidad de la captura. Relacionar en el formato, un aviso de privacidad que incorpore la autorización del tratamiento de los datos.

Para que la OCBP 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. Validar que en el aviso de privacidad se encuentren todas las finalidades de tratamiento asociadas a la captura de los datos solicitados

## 6. **NORMATIVA APLICABLE**

- Constitución Política, Artículo 15.
- Ley 1266 de 2008.
- Sentencia C – 1011 de 2008.
- Decretos Reglamentarios 1727 de 2009 y 2952 de 2010.
- Sentencia C - 748 del 2011.
- Ley 1581 de 2012.
- Decreto Reglamentario Parcial 1377 de 2013.
- Ley 1712 de 2014.
- Decretos Reglamentarios 103 y 1081 de 2015.
- 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.
- Decreto 620 de 2020 el cual determina en materia de Protección y Tratamiento De Datos Personales, las bases y medidas necesarias que deben adoptar las entidades públicas en el manejo de los datos digitales.
- NTC-ISO/IEC 27001- 27002:2022: norma internacional para los sistemas de gestión de la seguridad de la información. (SGSI)

## 7. **DESARROLLO PRIMARIO**

### 7.1 **PRINCIPIOS PARA EL TRATAMIENTO DE DATOS PERSONALES**

**PRINCIPIO DE LEGALIDAD:** El tratamiento de Datos es una actividad reglada, la cual deberá estar sujeta a las disposiciones legales vigentes y aplicables que rigen el tema.

**PRINCIPIO DE FINALIDAD:** La actividad de tratamiento de Datos Personales que realice La OCBP o a la cual tuviere acceso, obedecerán a una finalidad legítima en consonancia con los principios constitucionales, y ésta deberá ser informada al respectivo TITULAR de los Datos Personales.

**PRINCIPIO DE LIBERTAD:** El tratamiento de los Datos Personales sólo puede realizarse con el consentimiento, previo, expreso e informado del TITULAR. Los Datos Personales no podrán ser obtenidos o divulgados sin previa autorización del TITULAR; o en ausencia de Mandato Legal, Estatutario o Judicial que releve el consentimiento otorgado por el TITULAR.

**PRINCIPIO DE VERACIDAD O CALIDAD:** La información sujeta a Tratamiento de Datos Personales debe ser Veraz, Completa, Exacta, Actualizada, Comprobable y Comprensible. Se prohíbe el Tratamiento de Datos parciales, incompletos, fraccionados o que induzcan a error.

**PRINCIPIO DE TRANSPARENCIA:** En el tratamiento de Datos Personales, se garantizará al TITULAR su derecho de obtener en cualquier momento y sin restricciones, información acerca de la existencia de cualquier tipo de información o Dato Personal que sea de su interés o TITULARIDAD.

**PRINCIPIO DE ACCESO Y CIRCULACIÓN RESTRINGIDA:** El tratamiento de Datos Personales se sujeta a los límites que se derivan de la naturaleza de éstos, de las disposiciones de la ley y la Constitución. En consecuencia, el tratamiento de los Datos Personales sólo podrá hacerse por personas autorizadas por el TITULAR y/o Terceros Autorizados conforme a la ley.

Los Datos Personales, salvo la información pública, no podrán estar disponibles en internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los TITULARES o Terceros Autorizados conforme a la ley.

**PRINCIPIO DE SEGURIDAD:** La información sujeta a tratamiento se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros, evitando la adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento a los Datos Personales.

**PRINCIPIO DE CONFIDENCIALIDAD:** Toda persona, natural o jurídica, que administre, maneje, actualice o tenga acceso a información de cualquier tipo, que se encuentre en Bases de Datos, está obligada a garantizar la reserva de la información; por lo que, la persona que maneje este tipo de información, se compromete a conservar y mantenerla, de manera estrictamente confidencial, quedándole vedada la actitud de revelar a terceros la información que llegare a conocer en la ejecución y ejercicio de sus funciones. Lo anterior encuentra excepción cuando se trate de actividades autorizadas expresamente, por la ley de protección de Datos. Esta obligación persiste y se mantendrá, inclusive, después de finalizada la relación con las labores que comprenden el Tratamiento de los Datos.

### 7.2 **RESPONSABLE DEL TRATAMIENTO Y ÁMBITO DE APLICACIÓN**

En esta política se define como el responsable del tratamiento de Datos Personales a la ORGANIZACIÓN CLÍNICA BONNADONA PREVENIR S.A.S., la cual se encuentra identificada con Nit. 800.194.798 -2, domiciliada en la Carrera 49 C # 82 – 65, de Barranquilla, Colombia, y podrá ser contactada a través del PBX 57 3770055 o en la dirección de correo electrónico [siau@bonnadona.co](mailto:siau@bonnadona.co); para los efectos, también se tendrá en cuenta como medio informativo la página web de la OCBP, [www.organizacioncbp.org](http://www.organizacioncbp.org).

### 7.3 **AUTORIZACIONES**

La OCBP requiere la autorización previa, informada y expresa del TITULAR, la cual será obtenida por medios físicos, electrónicos o mediante conductas inequívocas del titular que lleven a concluir razonablemente a se ha otorgado la autorización respectiva de tal manera que pueda ser objeto de tratamiento posterior.

La OCBP se compromete a que al solicitar la información al TITULAR se debe informar de manera clara, la finalidad para la cual se recaudan los Datos Personales; además, se debe indicar el tratamiento al cual pueden ser sometidos los Datos Personales, los derechos y los medios a través

de los cuales puede ejercerlos y la facultad de autorizar o no el tratamiento en caso de Datos sensibles.

La OCBP no requiere autorización del TITULAR de los Datos Personales cuando se verifiquen las siguientes situaciones:

1. Responder a una orden judicial, cuando los solicita una entidad pública o administrativa en ejercicio de sus funciones legales.
2. Cuando los Datos Personales sean de naturaleza pública.
3. En casos de urgencia médica o sanitaria.
4. Cuando la información autorizada, sea determinada por la ley como de fines históricos, estadísticos o científicos.
5. Cuando sean Datos relacionados con el registro civil de las personas.

#### AUTORIZACIÓN DE DATOS DE MENORES DE EDAD

El tratamiento de Datos Personales de niños, niñas y adolescentes está prohibido, excepto cuando se trate de Datos de naturaleza pública, y cuando dicho tratamiento cumpla con los siguientes parámetros y requisitos:

1. Que responda y respete el interés superior de los niños, niñas y adolescentes.
2. Que se asegure el respeto de sus derechos fundamentales.

Cumplidos los anteriores requisitos, el representante legal del niño, niña o adolescente otorgará la autorización, previo al ejercicio del menor de su derecho a ser escuchado. La opinión otorgada por el niño, niña o adolescente, será valorada teniendo en cuenta la madurez, autonomía y capacidad para entender el asunto. La OCBP se compromete a salvaguardar con celo la privacidad, confidencialidad y seguridad de los Datos de los menores de edad.

#### FORMATO DE AUTORIZACIÓN PARA EL TRATAMIENTO INSTITUCIONAL DE DATOS PERSONALES POR PARTE DE PACIENTES Y/O USUARIOS

Manifiesto que OTORGO mi consentimiento de forma libre y voluntaria a ORGANIZACIÓN CLINICA BONNADONA PREVENIR S.A.S. (en adelante OCBP) para que trate mi información personal o de mi familiar menor de edad de acuerdo con la Política de Tratamiento de Datos Personales dispuesta por la sociedad de manera física y electrónica en la web [www.organizacioncbp.org](http://www.organizacioncbp.org) y a través de otros medios, la cual se me dio a conocer antes de recolectar mis datos personales. Manifiesto que me informaron que la recolección y uso de la información sensible mía o de mi familiar menor de edad, que corresponde a aquella que afecta la intimidad del titular, cuenta con el derecho de contestar o no las preguntas que me formulen y a entregar o no los datos solicitados. Manifiesto que me informaron que los datos sensibles que se recolectarán serán utilizados para el desarrollo del objeto social de la compañía en lo que tiene que ver con el diagnóstico, tratamiento y recuperación de la SALUD, compartir la información con las Entidades Administradoras de Planes de Beneficio, SOAT, IPS, auditorías externas y demás entidades o entes del sistema de salud para tratamientos médicos autorizados; gestionar tramites quejas y reclamos; cumplir con el SARLAFT; contactarla mediante aplicaciones de mensajería, email, teléfono o personalmente, para invitaciones a eventos, ofrecerle nuevos servicios, hacer encuestas de satisfacción del servicio ofrecido, confirmar datos personales, envío de noticias relacionadas con campañas de fidelización, mejora de servicio, programas, aplicativos, cambios de la políticas establecidas en la Organización y todo lo relacionado con la relación contractual y extracontractual que existe entre las partes y realizar estudios científicos o de investigación.

Manifiesto que me dieron a conocer los derechos sobre mis datos personales, los cuales versan de la siguiente manera:

(i) Conocer integralmente y de forma gratuita mis datos personales informados a la OCBP; (ii) Ser informado del uso que se dé a mis datos personales; (iii) Conocer el uso que se le da a mis datos personales, previa solicitud a OCBP; (iv) Solicitar prueba de la autorización otorgada a OCBP, salvo cuando expresamente se exceptúe como requisito para el tratamiento, de conformidad con la ley; (v) Revocar la autorización y/o solicitar la supresión de los datos cuando no se respeten los principios, derechos y garantías consagradas en la Ley; (vi) Presentar peticiones, quejas y reclamos ante las autoridades competente.

Declaro que me informaron que la responsable del tratamiento de datos personales (recolectar, almacenar y usar) en virtud de lo estipulado en la Ley 1581 de 2012 y sus decretos reglamentarios es la OCBP. Manifiesto que como titular del dato, mis derechos son los previstos en la constitución, en la Ley 1581 de 2012 y sus decretos reglamentarios, y en los derechos y deberes del paciente institucionalizados en la Organización, los cuales podré ejercer a través de los medios de comunicación oficina de SIAU, página web, y al email [siau@bonnadona.co](mailto:siau@bonnadona.co), línea de atención telefónica nacional 3770055.

NOMBRE TITULAR y/o REPRESENTANTE LEGAL

\_\_\_\_\_

FIRMA:

\_\_\_\_\_

IDENTIFICACIÓN: \_\_\_\_\_

FECHA:

#### 7.4 MANEJO DE DATOS PERSONALES Y SENSIBLES CON PROVEEDORES

En la OCBP, reconocemos la importancia crítica de salvaguardar la privacidad y seguridad de los datos sensibles que manejamos en nuestras operaciones diarias. Como parte de nuestra sólida política de gestión de datos, hemos implementado cláusulas contractuales específicas destinadas a garantizar que los datos sensibles compartidos entre nuestra empresa y nuestros proveedores estén protegidos de manera adecuada

y cumpliendo con las leyes y regulaciones aplicables en el territorio nacional. Debido a ello la cláusula contractual implementada es la siguiente:

## **CLÁUSULA 2 - CUMPLIMIENTO DE LA REGULACIÓN SOBRE DATOS PERSONALES:**

1. Las Partes aceptan que a las operaciones objeto de este Contrato en las que se incluyan datos de información personal registrados en bases de datos les son aplicables las disposiciones sobre datos personales.
2. Las Partes trabajarán, cada una en lo que corresponde a sus obligaciones, con el mayor cuidado posible para que dicha normatividad sea observada. Las Partes se comprometen, cada una con el otro, a colaborar para que a las Partes les sea posible respetar sus deberes en este ámbito.
3. Las Partes entienden que Organización Clínica Bonnadona Prevenir será el Responsable del Tratamiento y el Contratista será el Encargado del Tratamiento y cada uno le garantiza al otro que cumplirá con sus obligaciones legales en dicha calidad, de acuerdo con la ley 1581 de 2012.
4. El Contratista se obliga a realizar toda su gestión dentro de lo que la normatividad sobre datos personales permite y, en particular, a que los datos que reciba del contratante no los usará, guardará, compartirá, permitirá acceso a terceros de ninguna manera diferente de lo previsto en este contrato.

La implementación de esta cláusula contractual es una de las herramientas usadas para garantizar que todos los datos sean tratados con la debida diligencia y cuidado que merecen. Desde la OCBP Continuaremos revisando y actualizando nuestras políticas y cláusulas contractuales para mantenernos alineados con las mejores prácticas y las cambiantes regulaciones de protección de datos.

## **8. DERECHOS Y DEBERES DEL TITULAR**

En el tratamiento y protección de Datos Personales, los TITULARES tendrá los siguientes derechos y deberes; sin perjuicio de otros, derechos y deberes, previstos en las disposiciones que regulen o lleguen a regular esta materia:

1. El TITULAR tiene derecho a ser informado sobre el uso que se le da a sus Datos Personales.
2. El TITULAR tendrá derecho a conocer, rectificar, actualizar o revocar la autorización del tratamiento de sus datos personales.
3. El TITULAR tendrá derecho a solicitar prueba de la autorización otorgada al Responsable del Tratamiento salvo cuando expresamente se exceptúe como requisito para el Tratamiento, de conformidad con lo previsto en el artículo 10 de la mencionada ley.
4. El TITULAR tiene derecho a presentar consultas e interponer quejas, o solicitar el retiro de los Datos por incumplimiento en la normatividad y a acceder de manera gratuita a los Datos Personales, que hayan sido objeto de tratamiento.
5. El TITULAR debe garantizar la veracidad de la información que proporciona a la OCBP. Si la información resulta ser falsa, la OCBP se exime de la responsabilidad que se pueda ocasionar por la debida utilización de los Datos en los procesos que se validen.
6. El TITULAR se obliga a actualizar su información de manera oportuna.
7. El TITULAR tendrá derecho a presentar ante la Superintendencia de Industria y Comercio quejas por infracciones a lo dispuesto en la presente ley y las demás normas que la modifiquen, adicionen o complementen.
8. La revocatoria y/o supresión procederá cuando la Superintendencia de Industria y Comercio haya determinado que en el Tratamiento el Responsable o Encargado han incurrido en conductas contrarias a esta ley y a la Constitución.

### **8.1 DEBERES DE LA ORGANIZACIÓN CLINICA BONNADONA PREVENIR COMO RESPONSABLE DE LOS DATOS PERSONALES**

En el tratamiento y protección de Datos Personales, la OCBP específicamente el área Jurídica en conjunto con Sistemas, tendrán los siguientes deberes; sin perjuicio de otros deberes previstos en las disposiciones que regulen o lleguen a regular esta materia:

1. Garantizar al TITULAR, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data.
2. Solicitar y conservar copia de la autorización otorgada por el TITULAR, para el tratamiento de Datos Personales.
3. Informar debidamente al TITULAR, sobre la finalidad de la recolección de los Datos Personales y los derechos que le asisten en virtud de la autorización otorgada.
4. Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
5. Garantizar que la información sea veraz, completa, exacta, actualizada, comprobable y comprensible.
6. Actualizar oportunamente la información, atendiendo de esta forma todas las novedades respecto de los Datos del TITULAR. Adicionalmente, se deberán implementar todas las medidas necesarias para que la información se mantenga actualizada.
7. Rectificar la información cuando sea incorrecta y comunicar lo pertinente.
8. Respetar las condiciones de seguridad y privacidad de la información del TITULAR.
9. Tramitar las consultas y reclamos formulados en los términos señalados por la ley.
10. Identificar cuando determinada información se encuentra en discusión por parte del TITULAR.
11. Informar a solicitud del TITULAR sobre el uso dado a sus Datos.
12. Informar a la autoridad de protección de Datos cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los TITULARES.
13. Cumplir los requerimientos e instrucciones que imparta la Superintendencia de Industria y Comercio sobre el tema en particular.
14. Usar únicamente Datos cuyo tratamiento esté previamente autorizado de conformidad con lo previsto en la ley 1581 de 2012.
15. Velar por el uso adecuado de los Datos Personales de los niños, niñas y adolescentes, en aquellos casos en que se entra autorizado el tratamiento de sus Datos.
16. Registrar en la base de Datos la leyenda "reclamo en trámite" en la forma en que se regula en la ley.
17. Insertar en la base de Datos la leyenda "información en discusión judicial" una vez notificado por parte de la autoridad competente sobre procesos judiciales relacionados con la calidad del dato personal.
18. Abstenerse de circular información que esté siendo controvertida por el TITULAR y cuyo bloqueo haya sido ordenado por la Superintendencia de Industria y Comercio

19. Permitir el acceso a la información únicamente a las personas que pueden tener acceso a ella.
20. Usar los Datos Personales del TITULAR sólo para aquellas finalidades para las que se encuentre facultada debidamente y respetando en todo caso la normatividad vigente sobre protección de Datos Personales.
21. **TIPO DE INFORMACION REGISTRADA**

**DATOS PÚBLICOS:** La OCBP, advierte que trata sin previa autorización del titular los datos personales de naturaleza pública y los contenidos en los registros públicos. Esta situación implica que no se adopten las medidas necesarias que garanticen el cumplimiento de los otros principios y obligaciones contempladas en la Ley 1581 de 2012 y demás normas que regulen esta materia.

**DATOS PERSONAL:** Es cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. La información personal recopilada puede incluir, pero no limitarse a:

Nombre, direcciones y números de teléfono

Fecha y lugar de nacimiento, así como su género

Direcciones de correo electrónico.

Información necesaria para facilitar el contacto u otros servicios, incluyendo información familiar o laboral.

Número de cédula, pasaporte, nacionalidad y país de residencia

Identificación, representación y existencia en caso de personas jurídicas

Uso de servicios.

Información personal brindada a través de encuestas u otros métodos de investigación.

Información personal brindada a la oficina de Atención al Usuario.

Por la naturaleza de nuestra institución prestadora de servicios de salud, también registramos Datos básicos de la persona responsable del paciente, así como la entidad promotora de salud a la que se encuentra afiliado.

**DATOS SENSIBLES:** La OCBP restringirá el tratamiento de datos personales sensibles a lo estrictamente indispensable y solicitará consentimiento previo y expreso a los titulares informando sobre la finalidad exclusiva de su tratamiento

La OCBP utiliza y trata datos catalogados como sensibles, cuando:

1. El Titular haya dado su autorización explícita a dicho tratamiento, salvo en los casos que por ley no sea requerido el otorgamiento de dicha autorización.
2. El Tratamiento sea necesario para salvaguardar el interés vital del Titular y este se encuentre física o jurídicamente incapacitado. En estos eventos, los representantes legales deberán otorgar su autorización.
3. El Tratamiento se refiera a datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.
4. El Tratamiento tenga una finalidad histórica, estadística o científica. En este evento deberán adoptarse las medidas conducentes a la supresión de identidad de los Titulares
5. Cuando el tratamiento de esta clase de información sea posible, la OCBP se compromete con cada titular de datos de información en anunciarle en el momento de la recolección de los datos, cuáles de los datos que serán objeto de tratamiento son de carácter sensible y la finalidad de su tratamiento. A su vez, la OCBP se obliga a reforzar los niveles de seguridad frente al tratamiento de este tipo de datos y aumentar la restricción en su acceso y uso, para un tratamiento adecuado de los mismos.

En adición a lo anterior, la OCBP cumple con las siguientes obligaciones:

1. Informar al titular que cuando se trate de datos sensibles no estará obligado a autorizar su tratamiento.
2. Informar al titular de forma explícita y previa de los requisitos generales de la autorización para la recolección de cualquier tipo de dato personal, cuáles datos objeto de Tratamiento son de carácter sensible y la finalidad del tratamiento y obtener el consentimiento expreso
3. No condicionar ninguna actividad a que el titular suministre datos personales sensibles (salvo de que exista una causal legal o contractual para hacerlo).

Cuando el tratamiento de los datos personales sensibles insertos en las Historias Clínicas de los pacientes se realizará teniendo en cuenta los principios descritos en el presente manual y consagrados en la Ley que orientan la política de tratamiento de datos personales, los cuales se aplicarán e interpretarán en armonía con los lineamientos prescritos en la regulación especial contemplada en la Resolución 1995 de 1999 para el manejo de la Historia Clínica y demás normas que desarrollen, complementen, modifiquen o sustituyan dicha norma. Para el efecto, se tendrá en cuenta que la Historia Clínica se encuentra sometida a reserva legal y solo podrá ser conocida con previa y expresa autorización de cada paciente o en los demás casos en que la Ley lo autorice.

**TRATAMIENTO DE DATOS DE MENORES:** En el tratamiento de datos personales, la OCBP asegurará el respeto a los derechos prevalentes de los niños, niñas y adolescentes. El representante legal o tutor del niño otorgará la autorización, previo ejercicio del menor de su derecho a ser escuchado, se tendrá en cuenta la voluntad del menor titular considerando su capacidad de autodeterminación, madurez y capacidad de entender las finalidades del tratamiento de su información personal y las consecuencias del mismo.

Todo responsable y encargado involucrado en el tratamiento de los datos personales de niños, niñas y adolescentes, deberá vigilar el uso adecuado de los mismos. Para este fin deberán aplicarse los principios y obligaciones establecidos en la Ley 1581 de 2012; asimismo la familia y la sociedad deben velar porque los responsables encargados del tratamiento de los datos personales de los menores de edad cumplan con las obligaciones establecidas en la mencionada Ley.

**TRATAMIENTO EN SISTEMAS DE VIDEO VIGILANCIA:** La OCBP utiliza diversos medios de video vigilancia instalados en diferentes sitios internos y externos de sus instalaciones u oficinas, informando sobre la existencia de estos mecanismos mediante la difusión de sitios visibles de anuncios de video vigilancia.

La información recolectada se utilizara para fines de seguridad de los bienes, instalaciones y personas que se encuentren es éstas. Esta



información puede ser usada como prueba en cualquier tipo de proceso ante cualquier tipo de autoridad y organización con sujeción y cumplimiento de las normas aplicables.

Las imágenes solo serán tratadas cuando sean adecuadas, pertinentes y no excesivas en relación con el ámbito y las finalidades determinadas, legítimas y explícitas que hayan justificado la instalación de las cámaras o videocámaras. En cualquier caso el uso de sistema de video-vigilancia será respetuoso protegiendo el derecho a la intimidad de las personas. Las imágenes serán conservadas por el tiempo necesario de acuerdo a la finalidad para la que se recolectan.

**TRATAMIENTO DE DATOS BIOMÉTRICOS:** La OCBP utiliza dispositivos de recolección de datos biométricos, cuya finalidad se limitará a realizar labores de autenticación y/o enrolamiento de usuarios, ejecutar controles de suplantación, y controlar el acceso a sus instalaciones.

## 10. CLASIFICACIÓN DE BASES DE DATOS EN LA ORGANIZACIÓN CLÍNICA BONNADONA PREVENIR S.A.S Y FINALIDAD.

### BASE DE DATOS DE LOS PACIENTES

Son las bases de datos físicas o automatizadas que se encuentran estructuradas, y que contienen datos de naturaleza pública y privada de personas naturales en calidad de pacientes y usuarios. La OCBP da a conocer a sus usuarios y pacientes el uso y tratamiento de sus datos personales.

La OCBP utiliza la información de sus pacientes para asegurar la prestación de servicios de salud, facturar y cobrar ante las personas naturales o jurídicas responsables del pago, diligenciamiento del Registro Individual de la Prestación de Servicios de Salud (RIPS), reporte de información solicitada por normatividad legal, fines administrativos tales como auditorías, facturación, contabilidad y con el consentimiento del titular de la información podrá adelantar procesos de investigación, estadísticas, campañas de prevención y promoción y, en general para utilizarla en políticas de salud pública.

#### Finalidad

1. Realizar actividades relacionadas con la prestación de servicios de salud en desarrollo de las actividades y objeto social de la Clínica, como por ejemplo, pero sin limitarse, atención en salud, actividades corporativas, administrativas, de información, comercialización, petición, recaudo, cobranza, así como para actividades que provengan de los trámites propios del Sistema de Seguridad Social en Salud y del cumplimiento de las normas que lo regulan.
2. Contactar a los pacientes a través de medios telefónicos, físicos, personales y/o electrónicos (como SMS, chat, correo electrónico y demás medios que así puedan considerarse).
3. Crear y gestionar bases de datos (incluyendo bases de datos en relación con los datos sensibles) para la prestación de los servicios propios de la Clínica, fines de investigación, desarrollo de servicios y/o productos, estudios de riesgo y cálculos actuariales. La OCBP no comparte esta información con ninguna persona ajena o no autorizada de acuerdo con la legislación y la jurisprudencia vigente; no obstante, podrá compartirse o suministrarse información con las autoridades judiciales o administrativas que en ejercicio de sus atribuciones legales lo soliciten o con autoridades sanitarias.
4. Enviar notificaciones de cambios o mejoras en la prestación de servicios y publicidad sobre los mismos, de acuerdo con la legislación aplicable, así como enviar información de revistas o temas del sector salud que consideremos puedan ser de su interés.
5. Prestación de servicios de salud.
6. Información sobre campañas de promoción y planes de prevención en salud Procesar, confirmar y cumplir con el objeto misional de la OCBP o algún otro servicio que el TITULAR solicite.
7. La OCBP puede utilizar esta información para fines administrativos y analíticos; tales como administración de sistemas de información, facturación, contabilidad y auditorías, relacionamiento comercial, procesamiento y verificación de medios de pago, correspondencia de nuestra área de Atención al Usuario, y/o para el funcionamiento de los programas promocionales que se llagasen a implementar.
8. Realizar programas con los TITULARES de Datos Personales existentes.
9. Fomentar la investigación en los campos relacionados con la salud y nuestro objeto social.

### BASE DE DATOS DE LOS PROVEEDORES

Son las bases de datos físicas o automatizadas que contienen datos de las personas naturales o jurídicas que mantienen un vínculo contractual y comercial, cuyo tratamiento tiene como finalidad cumplir con las disposiciones contractuales estipuladas por la OCBP, para la adquisición de servicios y bienes demandados por ella para su normal funcionamiento o el cumplimiento de algunas de sus funciones. Esta base de datos contiene datos personales públicos, privados y sensibles, los cuales tienen como finalidad el desarrollo de relaciones contractuales. El tratamiento de estos datos para fines diferentes al mantenimiento de la relación contractual o el cumplimiento de deberes de carácter legal, requiere de autorización previa del titular. Conocimiento de SARLAFT Autorización expresa para el tratamiento de datos personales de proveedores.

#### Finalidad

La OCBP utiliza la información de sus proveedores para:

1. Mantener una eficiente comunicación de la información que sea de utilidad en los vínculos contractuales en los que sea parte el proveedor titular de la información
2. Informar las modificaciones internas de cualquier tipo que se presenten en desarrollo de los vínculos contractuales con el proveedor de la información
3. Evaluar la calidad de los servicios ofrecidos por el proveedor titular de la información.
4. Dar cumplimiento de las obligaciones contraídas por las sociedades con los proveedores titulares de la información.

5. Envío de invitaciones a contratar y realización de gestiones para las etapas precontractual, contractual y pos contractual.
6. Envío de invitaciones a eventos programados por la OCBP.
7. Las finalidades establecidas específicamente en las autorizaciones que sean otorgadas por los propios proveedores, cuando éstas se requieran de conformidad con la normatividad vigente o de conformidad con la Ley 1581 del 2012.
8. La OCBP podrá recolectar datos personales de los empleados de sus proveedores cuando por motivos de seguridad deba analizar y evaluar la idoneidad de determinadas personas, atendiendo las características de los servicios que se contraten con el proveedor. La recolección de los datos personales de empleados de los proveedores por parte de la OCBP, tendrá como finalidad verificar la idoneidad moral y competencia de los empleados; por tanto, una vez verificado este requisito, la OCBP devolverá tal información al proveedor, salvo cuando se autorice expresamente su conservación. Cuando la OCBP entregue datos personales de cualquier Titular a sus proveedores, éstos deberán proteger los datos personales suministrados, conforme lo dispuesto en las normas vigentes. La OCBP verificará que los datos solicitados sean necesarios, pertinentes y no excesivos respecto de la finalidad que fundamente la solicitud de acceso a los mismos.
9. Creación de terceros para efectos contables y tributarios.
10. Radicación y pago de facturas.
11. Dar soporte y respuesta a los requerimientos o solicitudes de los proveedores titulares.

## **BASE DE DATOS DE LOS COLABORADORES**

Son bases de datos físicas o automatizadas que contienen datos de las personas naturales que se vinculan laboralmente con la OCBP cuyo tratamiento tiene como finalidad cumplir con las disposiciones legales y reglamentarias. En esta base de datos se incorporan tanto información privada, pública, datos sensibles y de menores. El tratamiento de los datos para los fines diferentes a las obligaciones derivadas de la relación laboral requerirá autorización previa del titular o su representante legal, según sea el caso. En ningún caso, la OCBP dará tratamiento a los datos sensibles de menores de edad sin autorización previa.

### **Finalidad**

1. Permitir el ejercicio de sus derechos como empleado, establecidos en el Código Sustantivo del Trabajo y en las demás normas aplicables a la materia.
2. Enviar información de la OCBP, incluyendo invitaciones a eventos, boletines trimestrales (presentación de resultados), informe anual, y aquellas comunicaciones relacionadas con las actividades que adelanta.
3. Emitir certificaciones relativas a su condición de empleado, tales como certificados de ingresos y retenciones, constancias laborales, entre otros
4. Compartir información con proveedores con los que la OCBP desarrolle actividades en cumplimiento de su objeto social, con las limitaciones y las reglas establecidas por la OCBP.
5. Realizar proceso de selección y contratación, así como afiliaciones y pago al sistema de Seguridad Social, procesar nómina y realizar actividades de bienes y capacitación.
6. Actividades de seguridad y monitoreo a través del uso de la información biométrica y del registro de la huella.
7. Historiales de acceso a internet.
8. Foto para uso de identificación interna y campañas de socialización.
9. Procesos jurídicos y administrativos.
10. Los datos correspondientes a personas cuya relación laboral ha finalizado, se continuarán almacenando para los fines autorizados y bajo las mismas condiciones y niveles de seguridad.

### **Finalidad del tratamiento de datos de candidatos.**

Los datos suministrados por los interesados en las vacantes de la OCBP y la información personal obtenida del proceso de selección, se limita a la relacionada con su participación en el mismo; por tanto, su uso para fines diferentes está prohibido.

### **Finalidad del tratamiento de datos de excolaboradores.**

La OCBP almacenará los datos personales de todos los Empleados que hayan terminado su relación laboral. Este archivo tendrá como finalidad:

1. Servir como base para la expedición de los certificados laborales de que trata el Artículo 57, numeral 7° del Código Sustantivo del Trabajo, a solicitud del Exempleado o sus causahabientes.
2. Servir de base para el otorgamiento de referencias laborales a potenciales empleadores del Exempleado, cuando éste así lo autorice al momento de su desvinculación de cualquiera de Las Sociedades.
3. La información almacenada en este archivo podrá ser estudiada, analizada y utilizada por la OCBP a efectos de considerar al Exempleado en los procesos de contratación de personal que lleven a cabo.
4. Por otra parte, con ocasión de los eventos, capacitaciones o demás actividades llevadas a cabo por éstas, podrán grabar y tomar audios, videos o fotos de los empleados, en desarrollo de éstos. Estos audios, videos o fotos podrán ser utilizados por la OCBP en boletines, informes sectoriales, publicaciones, y en general en cualquier actividad de la OCBP, incluso una vez el empleado se retire de trabajar con la OCBP, es decir una vez la persona sea considerada como un ex empleado.

## **FORMATO DE AUTORIZACIÓN PARA EL TRATAMIENTO DE DATOS PERSONALES COLABORADORES**

ORGANIZACION CLINICA BONNADONA PREVENIR S.A.S. será el Responsable del tratamiento y, en tal virtud, podrá recolectar, almacenar, usar para las siguientes finalidades:

## DECLARACIONES

Manifiesto que me informaron que en caso de recolección de mi información sensible (o de mi familia), tengo derecho a contestar o no las preguntas que me formulen y a entregar o no los datos solicitados. Entiendo que son datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar discriminación por orientación política, convicciones religiosas o filosóficas, datos relativos a la salud, a la vida sexual y los datos biométricos). Manifiesto que me informaron que los datos sensibles que se recolectarán serán utilizados para las finalidades señaladas en este documento.

## DERECHOS DEL TITULAR

Sus derechos como titular del dato son los previstos en la Constitución y en la Ley 1581 de 2012 y sus decretos reglamentarios, especialmente los siguientes:

FINALIDAD	AUTORIZA	
	SI	NO
Efectuar las gestiones pertinentes para el desarrollo del objeto social de la compañía		
Manejo de mi hoja de vida, solicitud de convalidación de mi título académico y confirmación de mis referencias personales y familiares, afiliaciones a seguridad social.		
Gestionar trámites (solicitudes, quejas, reclamos).		
para consultar en las centrales de información de Sector Financiero CIFIN que administra la asociación bancaria y entidades financieras de Colombia y/o a cualquier otra entidad que maneje o administre base de datos para los mismos fines así como para que verifique en la lista internacional vinculante para Colombia de conformidad con el derecho internacional (lista de las Naciones Unidas), la lista emitida por la Oficina de Activos Extranjeros del Departamento del Tesoro de los Estados Unidos de América y aquellas otras listas o bases de datos públicas o privadas donde se relacionen personas presuntamente vinculadas a cualquier actividad ilícita		
Cumplir con las exigencias normativas del SARLAFT		
Cumplir con la normativa vigente en Colombia para empresas comerciales y del sector salud		
Efectuar encuestas de satisfacción respecto de los bienes y servicios ofrecidos por la Organización Clínica Bonnadona Prevenir S.A.S.		
Entregar información a entes certificadores de calidad sobre contratistas y empleados.		
Dar cumplimiento a las obligaciones contraídas por la Organización Clínica Bonnadona Prevenir S.A.S. con el Titular de la Información, con relación al pago de salarios, prestaciones sociales, sistema biométrico y demás retribuciones consagradas en el contrato de trabajo o según lo disponga la ley.		
Ofrecer programas de bienestar corporativo y planificar actividades empresariales, para el titular y sus beneficiarios (hijos, cónyuge, compañero permanente).		
Prestar los servicios ofrecidos por la Organización Clínica Bonnadona Prevenir S.A.S. y aceptados en el contrato suscrito.		
Suministrar la información a terceros con los cuales la Organización Clínica Bonnadona Prevenir S.A.S. tenga relación contractual y que sea necesario entregársela para el cumplimiento del objeto contratado.		

- a) Acceder en forma gratuita a los datos proporcionados que hayan sido objeto de tratamiento.
- b) Solicitar la actualización y rectificación de su información frente a datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o a aquellos cuyo tratamiento esté prohibido o no haya sido autorizado.
- c) Solicitar prueba de la autorización otorgada.
- d) Presentar ante la Superintendencia de Industria y Comercio (SIC) quejas por infracciones a lo dispuesto en la normatividad vigente.
- e) Revocar la autorización y/o solicitar la supresión del dato, a menos que exista un deber legal o contractual que haga imperativo conservar la información.
- f) Abstenerse de responder las preguntas sobre datos sensibles o sobre datos de las niñas y niños y adolescentes.

Estos derechos los podré ejercer a través de los canales o medios dispuestos por la ORGANIZACIÓN CLINICA BONNADONA PREVENIR para la atención al público, la línea de atención nacional 3770055, el correo electrónico [coordhumana@organizacioncbp.org](mailto:coordhumana@organizacioncbp.org), la oficina de gestión humana ubicada en la carrera 49c No. 82-65 de la ciudad de Barranquilla, cuya información puedo consultar en [www.organizacioncbp.org](http://www.organizacioncbp.org) disponibles para la atención de requerimientos relacionados con el tratamiento de mis datos personales y el ejercicio de los derechos mencionados en esta autorización. Por todo lo anterior, he otorgado mi consentimiento a ORGANIZACIÓN CLINICA BONNADONA PREVENIR S.A.S. para que trate mi información personal de acuerdo con la Política de Tratamiento de Datos Personales dispuesta por la sociedad en medio electrónico, a través de la página web [www.organizacioncbp.org](http://www.organizacioncbp.org), y a través de medios tecnológicos y que me dio a conocer antes de recolectar mis datos personales. Manifiesto que la presente autorización me fue solicitada y puesta de presente antes de entregar mis datos y que la suscribo de forma libre y voluntaria una vez leída en su totalidad.

**DECLARACIÓN DE ORIGEN DE BIENES E INGRESOS:** Con el fin de dar cumplimiento a las disposiciones legales vigentes y a los procedimientos de ORGANIZACION CLINICA BONNADONA - PREVENIR SAS sobre el Sistema Integral de Prevención de Lavado de Activos y Financiación del Terrorismo SARLAFT, de manera voluntaria declaro que todos los ingresos y demás activos que conforman mis ingresos no provienen de actividades ilícitas contempladas en el Código Penal Colombiano o en cualquier norma que lo modifique o adicione; que mis ingresos y demás activos no están destinados para financiar actividades terroristas; que mis bienes no se encuentra con registro negativo en listados de prevención de lavado de activos y financiación del terrorismo nacionales o internacionales.

Certifico a la ORGANIZACION CLINICA BONNADONA - PREVENIR SAS que no he permitido y me obligo a no permitir que terceras personas efectúen operaciones en cuanto a la relación o actividades a mi nombre con fondos provenientes de actividades ilícitas, y que no efectuaré transacciones destinadas a dar apariencia de legalidad a tales actividades, o en favor de personas relacionadas con las mismas. Declaro que la información que he suministrado a ORGANIZACION CLINICA BONNADONA - PREVENIR SAS es veraz y exacta, eximo a la entidad de cualquier responsabilidad proveniente de información que resultare ser errónea, falsa o inexacta y la autorizo a realizar los reportes pertinentes de conformidad a las disposiciones legales y que no hay en curso procesos de extinción de dominio sobre tales ingresos y demás activos.

**BIENES SUJETOS A EXTINCIÓN DE DOMINIO:** Los activos objeto de la relación contractual y/o comercial establecida con ORGANIZACION CLINICA BONNADONA - PREVENIR SAS (en adelante, "ORGANIZACION CLINICA BONNADONA - PREVENIR SAS"), no se encuentran incurso en las circunstancias consagradas en el artículo 16 la ley 1708 de 2014 sobre extinción de dominio.

**DEBER DE INFORMACIÓN:** me obligo a entregar a ORGANIZACION CLINICA BONNADONA - PREVENIR SAS la información veraz y verificable que este último le requiera para dar cumplimiento a la normatividad relacionada respecto a la prevención y control del riesgo de lavado de activos y financiación del terrorismo, así como a actualizar los datos suministrados cada vez que se considere pertinente. De la misma forma, informaré a ORGANIZACION CLINICA BONNADONA - PREVENIR SAS del inicio de cualquier proceso penal por los delitos de lavado de activos o financiación del terrorismo, sin importar si se encuentra en etapa de investigación o juicio, que lleve a cabo la autoridad competente en donde sea parte del proceso, así como cualquier citación que le realice dicha Autoridad para que comparezca dentro de una investigación o proceso penal relacionado con los mencionados delitos, sin importar en la calidad que sea citado.

**CUMPLIMIENTO DE LA LEY:** me comprometo a cumplir las obligaciones de las normas vigentes relacionadas con la prevención y control de lavado de activos y financiación de terrorismo mediante certificación suscrita por su representante legal.

NOMBRE TITULAR y/o REPRESENTANTE LEGAL \_\_\_\_\_

FIRMA: \_\_\_\_\_

ID: \_\_\_\_\_

FECHA: \_\_\_\_\_

## **BASE DE DATOS DE CLIENTES CONTRATANTES**

Son las bases de datos físicas o automatizadas que contienen datos de las personas naturales o jurídicas a las que le prestamos los servicios relacionados con nuestro objeto social, y con quienes ostentamos un vínculo contractual y comercial, cuyo tratamiento tiene como finalidad cumplir con las disposiciones contractuales estipuladas por la OCBP, para la prestación de los servicios ofrecidos por ella. Esta base de datos contiene datos personales públicos, privados y sensibles de clientes, potenciales clientes, empleados o personas de contacto de sus clientes, los cuales tienen como finalidad el desarrollo de relaciones contractuales. El tratamiento de estos datos para fines diferentes al mantenimiento de la relación contractual o el cumplimiento de deberes de carácter legal, requiere de autorización previa del titular. La OCBP da a conocer a sus Proveedores el uso y tratamiento de sus datos personales y conocimiento de SARLAFT Autorización expresa para el tratamiento de datos personales de proveedores.

### **Finalidad**

1. La OCBP podrá llevar a cabo el Tratamiento de la información personal acerca de sus Clientes para los propósitos de prestar los servicios profesionales por ellos contratados, de conformidad con el objeto social respectivo.
2. La OCBP asumirá que la información personal de terceros, cuyo Responsable sea el Cliente, que deba conocer La OCBP en razón o con ocasión de la prestación de los servicios contratados por el Cliente, ha sido tratada en apego estricto a lo dispuesto en la Ley 1581 y el Decreto 1377 de 2013. Lo anterior incluye que los datos de las mismas han sido tratados con autorización de su Titular, y que dicha autorización faculta al Cliente para procurar el Tratamiento de los datos por parte de La OCBP. En todo caso, los datos personales de terceros cuyo Responsable sea el Cliente serán tratados en el marco del objeto de los servicios contratados por el Cliente, a efectos de dar cumplimiento a la relación comercial que se haya entablado con el Cliente.
3. De igual manera, La OCBP podrá llevar a cabo el tratamiento de la información personal de sus Clientes actuales o futuros y de aquellos Clientes con los cuales haya terminado su relación comercial, con la finalidad de enviarles información comercial que a juicio de La OCBP pueda ser de su interés; así como, entre otros, invitarlos a eventos; emitir boletines, informes o publicaciones y en general, utilizar los datos para el desarrollo de las actividades comprendidas en el objeto social de La OCBP
4. Así mismo, La OCBP, con ocasión de los eventos, capacitaciones o demás actividades llevadas a cabo por ésta, podrá grabar y tomar audios, videos o fotos de Clientes del desarrollo de éstos. Estos audios, videos o fotos podrán ser utilizados por La OCBP en boletines, informes sectoriales, publicaciones, y en general en cualquier actividad de La OCBP.

## **BASE DE DATOS DE ACCIONISTAS**

Son bases de datos físicas o automatizadas que contienen datos e información personal de las personas naturales que ostentan la condición de accionista de La OCBP, se considera información reservada, pues la misma está registrada en los libros de comercio y tiene el carácter de reserva por disposición legal. La OCBP solo usará los datos personales de los accionistas para las finalidades derivadas de la relación estatutaria existente. La OCBP da a conocer a sus accionistas el uso y tratamiento de sus datos y conocimiento de SARLAFT y autorización expresa para el tratamiento de Datos Personales de Accionistas.

#### **Finalidad**

1. Permitir el ejercicio de los derechos derivados de la calidad de accionista, facilitando que estos puedan ejercer los derechos políticos y económicos establecidos en el Código de Comercio, en el Decreto 2555 de 2010, y en las demás normas aplicables a la materia.
2. Enviar información de La OCBP, incluyendo invitaciones a eventos, presentación de resultados, informe anual, y aquellas comunicaciones relacionadas con las actividades que adelanta La OCBP
3. Emitir certificaciones relativas a la relación del titular del dato con La OCBP, tales como certificados de renta, de participación accionaria, entre otros.
4. Compartir los datos personales con las compañías filiales y subsidiarias de La OCBP, para ofrecer productos y servicios. Estas compañías se podrán consultar en el Certificado de Existencia y Representación Legal de La OCBP
5. Compartir información con proveedores con los que La OCBP. desarrolle actividades en cumplimiento de su objeto social, con las limitaciones y las reglas establecidas por La OCBP

#### **BASE DE DATOS DE SISTEMA DE VIDEO VIGILANCIA**

Son bases de datos automatizadas que contienen información personal en forma de imágenes, videos de vigilancia y seguridad del personal que ingresa y/o transita por las instalaciones de la OCBP, cuya finalidad es garantizar controles de seguridad, verificar el cumplimiento por el colaborador, sus obligaciones y deberes laborales. La OCBP da conocer a los Titulares de la base de datos el uso y tratamiento de sus datos por medio de avisos de video vigilancia ubicados estratégicamente en las instalaciones de la misma.

#### **Finalidad**

1. Establecer controles de seguridad y acceso del personal a las instalaciones de la OCBP
2. Verificación de cuidado con los equipos de salud y cómputo por parte del personal a cargo.
3. Apoyar gestiones de atención al usuario.
4. Investigaciones por requerimiento de las autoridades.
5. Evaluación de protocolos de manejo de pacientes.
6. Evaluación de normas de bioseguridad en los procedimientos realizados en la Institución.
7. Cumplimiento del colaborador en sus obligaciones laborales.
8. **SEGURIDAD DE LA INFORMACIÓN**

La protección de la información no solo será responsabilidad del personal médico - asistencial, sino de todas las personas que tengan acceso a ella en la OCBP, en el ejercicio de sus funciones.

El personal médico, asistencial. Este personal humano accederá a Datos de naturaleza sensible porque el TITULAR de los mismos, de manera previa, expresa y voluntaria, le da a conocer esta información. Del mismo modo, en razón a su ejercicio profesional, tendrá conocimiento de la historia clínica del paciente. Teniendo en cuenta la protección exigida para este tipo de Datos, esta información será utilizada para los fines exclusivos de la prestación del servicio de salud y cualquier otro uso será considerado erróneo e ilegal.

Los colaboradores de la OCBP. Este personal humano se encuentra capacitado y asume con responsabilidad el tratamiento de los Datos de Sensibles, de los pacientes que son tratados en por la OCBP. A la vez, se encuentran advertidos sobre las obligaciones y sanciones que implica el uso inadecuado de los Datos Personales, al igual que son conocedores de los procedimientos contentivos en este manual, para el tratamiento de éstos, las restricciones y excepciones para el acceso a estos Datos, por parte de otras personas diferentes al TITULAR. También tienen conocimiento sobre la forma como los clasifican, comunican y entregan los Datos Personales. Además, conocen la importancia de no dejar expuestos resultados de carácter médico que puedan afectar la intimidad y privacidad de una persona, y de no utilizar los Datos Personales de los TITULARES, por fuera de la finalidad médica o administrativa establecida.

La OCBP cuenta con los siguientes mecanismos de seguridad para la salvaguarda de la información contenida en las bases de datos:

1. Capacitación del personal que ingresa a la Organización acerca de la Política de Tratamiento de datos personales, los mecanismos y protocolos de seguridad para el tratamiento de estos.
2. Ámbito de aplicación del procedimiento con especificación detallada de los recursos protegidos.
3. Medidas, normas, procedimientos, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en la Ley 1581 de 2012 y el Decreto 1377 de 2013.
4. Funciones y obligaciones del personal.
5. Estructura de las bases de datos de carácter personal y descripción de los sistemas de información que los tratan.
6. Procedimiento de notificación, gestión y respuesta ante las incidencias.
7. Procedimientos de realización de copias de respaldo y de recuperación de los datos.
8. Controles periódicos que se deban realizar para verificar el cumplimiento de lo dispuesto en el procedimiento de seguridad que se implemente.
9. Evitar la fuga de información sensible a través de análisis de correos y sus adjuntos a través del Firewall y software DLP (Data Loss Prevention).
10. La restricción en el uso de medios extraíbles (USB, CD, DVD).
11. Se autoriza el uso del botón de ImprimirPantalla por ser de uso operativo altamente utilizado para las labores diarias.
12. La protección ante malware o virus, contrarrestando los efectos de éstos con antivirus corporativo, para análisis en tiempo real

de documentos con código malicioso.

13. La Guarda los Datos Personales en servidores de dominio y aplicaciones donde se tienen perfiles de usuario, uso de contraseña segura y renovación periódica que aplica a todos los usuarios independientemente del cargo.
14. La restricción de ingreso al área de archivo y regida bajo procedimientos que propenden la protección de los Datos de intrusiones y/o pérdidas. El área de archivo cumple con condiciones y controles ambientales para la conservación de los archivos el tiempo estipulado por la ley.
15. Cuando el TITULAR no pueda presentarse personalmente a obtener sus resultados, envíe autorización escrita indicando el nombre de la persona autorizada, acompañada de fotocopia de la cédula de ciudadanía, tanto del TITULAR como de la persona autorizada. Ahora bien, si el TITULAR autoriza su envío por email o correo certificado, debe firmar el formato donde así lo indica, los anteriores documentos serán debidamente verificados, organizados y posteriormente archivados.
16. **TRANSFERENCIA Y TRANSMISIÓN DE DATOS PERSONALES**

La OCBP cumple con lo establecido en el artículo 26 de la Ley Estatutaria 1581 de 2012, y se abstiene de transferir Datos Personales de los TITULARES a otros países que no cuenten con iguales o superiores estándares de protección.

Sin embargo, procederá la transferencia y transmisión de Datos Personales en las siguientes excepciones:

1. Información respecto de la cual el TITULAR haya otorgado su autorización expresa e inequívoca para la transferencia.
2. Intercambio de Datos de carácter médico, cuando así lo exija el Tratamiento del TITULAR, por razones de salud o higiene pública.
3. Transferencias bancarias o bursátiles, conforme a la legislación que les resulte aplicable.
4. Transferencias acordadas en el marco de tratados internacionales, en los cuales la República de Colombia sea parte, con fundamento en el principio de reciprocidad.
5. **GOBIERNO EN LA PROTECCIÓN DE DATOS PERSONALES**

La OCBP dentro de su programa de protección de datos personales ha estructurado unos roles para el desarrollo, verificación y control de las políticas de privacidad, protección y tratamiento de datos personales, 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 OCBP 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 OCBP 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 OCBP 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 OCBP. 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.

El Gobierno en la Protección de Datos Personales está integrado por cada uno de los siguientes miembros:

- Director Jurídico.
- Director de Sistemas.
- Secretario General.

El nombramiento de estos integrantes será consagrado a través de Acta emanada por el comité institucional de Gerencia de la Información. Así mismo los cambios de estos será realizado a través del comité ya mencionado, constando en su respectiva acta.

#### 14. PROCEDIMIENTO PARA CONSULTA Y RECLAMOS

**Consultas:** Las consultas realizadas por el TITULAR o sus causahabientes podrán ser suministradas y atendidas por la OCBP en un término de (10) días hábiles, a partir del recibo de la solicitud. Este término podrá ser prorrogado por un término máximo de (5) días hábiles.

Con respecto a la atención de las solicitudes de consulta de Datos Personales la OCBP garantiza:

1. Los medios de comunicación electrónica, los cuales están habilitados en el correo de SIAU (Sistema de Información y Atención al Usuario) [siau@bonnadona.co](mailto:siau@bonnadona.co).
2. Oficina de SIAU ubicada en la Carrera 49C #82-65, entrada de urgencia pediátrica.
3. Recepción de la OCBP, primer piso, Torre AIDOC.

**Reclamos:** El TITULAR o sus causahabientes de Datos Personales, que consideren que la información contenida en la Base de Datos de la OCBP

debe ser objeto de corrección, actualización o supresión, o cuando adviertan el presunto incumplimiento por parte de cualquiera de los deberes contenidos en la ley o en esta política; ante lo anterior, éstos podrán presentar un reclamo ante el departamento Jurídico, el cual será tramitado bajo las siguientes reglas:

Solicitud dirigida al Departamento Jurídico de la OCBP, por correo convencional, a la Carrera 49C # 82 -65 en la recepción, con la identificación del TITULAR, la descripción de los hechos que dan lugar al reclamo, la dirección, y acompañando los documentos que se quieran hacer valer.

El término máximo para atender el reclamo será de quince (15) días hábiles contados, a partir del día siguiente a la fecha de su recibo, el cual se podrá prorrogar por un término máximo de ocho (8) días hábiles.

Si el reclamo resulta incompleto, se requerirá al interesado, dentro de los cinco (5) días hábiles siguientes a la recepción del reclamo, para que subsane las fallas. Si transcurridos dos (2) meses desde la fecha del requerimiento, sin que el solicitante presente la información requerida, se entenderá que ha desistido del reclamo.

Antes de acudir a la entidad encargada de vigilar el cumplimiento de las normas sobre protección de Datos personales, el TITULAR debe tramitar inicialmente su reclamo con la OCBP, a través de los medios y canales dispuestos para tal fin.

## 15. PROCEDIMIENTO DE MANEJO DE DATOS SENSIBLES SIN AVISO DE PRIVACIDAD O NOTIFICACIÓN DE LAS POLÍTICAS DE PRIVACIDAD.

La OCBP adoptará los siguientes lineamientos ante las eventualidades en las que le sean suministrados los datos sensibles de proveedores, colaboradores, pacientes y sus familiares, y no se les haya informado debidamente, por los medios dispuestos para ello, de las políticas de confidencialidad y aviso de privacidad.

- **Evaluar la situación:** Determinar los motivos por los cuales no se ha informado al titular sobre el aviso de privacidad. Esto podría ser debido a un error administrativo, una omisión involuntaria o cualquier otra razón. Entender la causa raíz ayudará a tomar medidas adecuadas.
- **Detener la divulgación no autorizada:** Si se ha detectado que se está manejando información sensible sin el consentimiento del titular y sin proporcionarle el aviso de privacidad correspondiente, es crucial detener cualquier divulgación adicional de estos datos de inmediato.
- **Notificar al titular:** Notificar al titular de los datos sobre el uso de su información sensible. Esta notificación debe incluir detalles sobre qué información se ha recolectado, con qué propósito y cómo se utilizará. Además, se debe proporcionar la oportunidad para que el titular otorgue o revoque su consentimiento.
- **Implementar medidas de seguridad adicionales:** En casos donde la información sensible se haya manejado sin el consentimiento del titular, es importante reforzar las medidas de seguridad para proteger esos datos. Esto puede incluir la encriptación de datos, el acceso restringido, la capacitación del personal sobre la privacidad de los datos, entre otras medidas.
- **Auditoría interna:** Realizar auditorías internas periódicas para garantizar el cumplimiento de los procedimientos de privacidad de datos. Esto puede ayudar a identificar y corregir cualquier brecha en el manejo de datos sensibles y evitar problemas futuros.
- **Transparencia y comunicación:** Mantener una comunicación abierta y transparente con los titulares de los datos sobre cómo se manejan y protegen su información sensible. Esto ayuda a construir confianza y demostrar el compromiso de la compañía con la privacidad de los datos.

## 16. SENSIBILIZACIÓN Y CAPACITACIÓN

Para la OCBP es muy importante tener actualizados a los colaboradores tanto administrativos como asistenciales sobre las disposiciones, políticas y reglamentación relacionada con la protección de los datos personales.

Para tal compromiso, la institución incorpora dentro de su programa de inducción y recapitación los principales conceptos, lineamientos y disposiciones prácticas sobre el tratamiento de los datos personales, el cual será complementada con la capacitación anual liderada por las áreas de Sistemas y Jurídica. 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 OCBP.

*Al final de cada sesión de capacitación, realiza una evaluación para medir la efectividad del programa. Esto puede incluir cuestionarios de conocimientos, discusiones grupales o ejercicios prácticos. Se realizarán feedbacks de los resultados de las evaluaciones y de eventualidades que transcurran en la Institución para mejorar el programa de capacitación y mantenerlo actualizado paralelamente con las necesidades de la organización.*

*Las capacitaciones serán programadas dos veces al año adecuadas a cada área, una destinada a los colaboradores administrativos y otra para el personal asistencial, toda vez que estos manejan enfoques diferentes en cuanto al tratamiento de datos personales.*

## 17. MODIFICACIONES Y VIGENCIA

Este Manual de políticas, protección y privacidad de Datos Personales de la Información de los TITULARES, empezará a regir desde el día 01 de enero de 2024, dentro del marco establecido por la ley

## 18. EVALUACION Y SEGUIMIENTO

La OCBP realizará procesos de evaluación para garantizar el cumplimiento y la adherencia del presente Manual a través de auditorías en materia de protección de datos personales verificando de manera directa y por medio de terceros, que las políticas y procedimientos se han implementado

adecuadamente en la institución.

Con base a los resultados obtenidos, se evalúa e implementa los planes de acción (preventivos, correctivos y de mejora) necesarios. Como norma general la OCBP realiza estos procesos de revisión con una periodicidad mínima de un año o de forma extraordinaria ante incidentes graves que afecten a la integridad de las bases de datos personales.

Los resultados de la revisión junto con los eventuales planes de mejora definidos, son presentados por el área de Sistemas y los asignados en el Gobierno de Protección de Datos Personales ante la Dirección Administrativa, para su valoración y aprobación.