MANUAL INTERNO DE SEGURIDAD

ÍNDICE

1. Base legal y ámbito de aplicación

OFTALMOS S.A., con objeto de garantizar el adecuado cumplimiento de la Ley Estatutaria 1581 de 2012 de Protección de Datos (LEPD) y del Decreto 1377 de 2013, adopta este Manual Interno de Seguridad donde se recogen las medidas técnicas, humanas y administrativas necesarias para otorgar seguridad a los registros con el fin de impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento, de acuerdo con el principio de seguridad recogido en el artículo 4 literal g) de la LEPD.

El presente manual pertenece a: OFTALMOS S.A..

- Dirección: AV Calle 100 N. 18A-51
- Correo electrónico: tusdatos@barraquer.com.co
- Teléfono: 2187077

Las disposiciones de este documento se aplican a las bases de datos objeto de responsabilidad de OFTALMOS S.A., así como a los sistemas de información, soportes y equipos empleados en el tratamiento de los datos, que deban ser protegidos de acuerdo con la normativa vigente, a las personas que participan en el tratamiento y a los locales donde se ubican dichas bases de datos.

2. Definiciones de conceptos en materia de seguridad

- **Acceso autorizado:** Autorización concedida a un usuario para el uso de determinados recursos. En dispositivos automatizados es el resultado de una autentificación correcta, generalmente mediante el ingreso de usuario y contraseña.
- **Autenticación:** Procedimiento de verificación de la identidad de un usuario.

- **Contraseña:** Seña secreta que permite el acceso a dispositivos, información o bases de datos antes inaccesibles. Se utiliza en la autentificación de usuarios que permite el acceso autorizado.

- **Control de acceso:** Mecanismo que permite acceder a dispositivos, información o bases de datos mediante la autentificación.

- **Copia de respaldo:** Copia de los datos de una base de datos en un soporte que permita su recuperación.

- **Identificación:** Proceso de reconocimiento de la identidad de los usuarios.

- **Incidencia:** Cualquier anomalía que afecte o pueda afectar a la seguridad de los datos, constituyendo un riesgo para la confidencialidad, disponibilidad o integridad de las bases de datos o de los datos personales que contienen.

- **Perfil de usuario:** Grupo de usuarios a los que se da acceso.

- **Recurso protegido:** Cualquier componente del sistema de información, como bases de datos, programas, soportes o equipos, empleados para el almacenamiento y tratamiento de datos personales.

- **Responsable de seguridad:** Una o varias personas designadas por el responsable del tratamiento para el control y la coordinación de las medidas de seguridad.

- **Sistema de información:** Conjunto de bases de datos, programas, soportes y/o equipos empleados para el tratamiento de datos personales.

- **Soporte:** Material en cuya superficie se registra información o sobre el cual se pueden guardar o recuperar datos, como el papel, la cinta de video, el CD, el DVD, el disco duro, etc.

- **Usuario:** Sujeto autorizado para acceder a los datos o recursos, o proceso que accede a los datos o recursos sin identificación de un sujeto.

3. Cumplimiento y actualización

El Manual Interno de Seguridad es un documento interno de la empresa de obligatorio cumplimiento para todo el personal de OFTALMOS S.A., con acceso a los sistemas de información que contengan datos personales.

Este manual debe ser sometido a permanente revisión y actualización siempre que se produzcan cambios en los sistemas de información, el sistema de tratamiento, la organización o el contenido de la información de las bases de datos, que puedan afectar a las medidas de seguridad implementadas. Asimismo, el manual debe adaptarse en todo momento a la normativa legal en materia de seguridad de datos personales.

4. Medidas de seguridad

Las bases de datos son accesibles únicamente por las personas designadas por OFTALMOS S.A., y referidas en el numeral 6 de este documento.

Los responsables de seguridad de OFTALMOS S.A., señalados en numeral 6 del presente manual, se encargan de gestionar los permisos de acceso a los usuarios, el procedimiento de asignación y distribución que garantiza la confidencialidad, integridad y almacenamiento de las contraseñas, durante su vigencia, así como la periodicidad con la que se cambian.

A continuación se enumeran y detallan las medidas de seguridad implementadas por OFTALMOS S.A..

4.1. Medidas de seguridad comunes

4.1.1. Gestión de documentos y soportes

Los documentos y soportes en los que se encuentran las bases de datos se determinan en el inventario de documentos y soportes.

Los encargados de vigilar y controlar que personas no autorizadas no puedan acceder a los documentos y soportes con datos personales son los usuarios autorizados para

acceder a estos. Los usuarios autorizados están referidos en el numeral 6 sobre bases de datos y sistemas de información del presente manual.

Los documentos y soportes deben clasificar los datos según el tipo de información que contienen, ser inventariados y ser accesibles solo por el personal autorizado, salvo que las características de los mismos hagan imposible la identificación referida, en cuyo caso se dejará constancia motivada en el registro de entrada y de salida de documentos y en el Manual Interno de Seguridad.

La identificación de los documentos y soportes de contengan datos personales sensibles debe realizarse utilizando sistemas de etiquetado comprensibles y con significado que permita a los usuarios autorizados identificar su contenido y que dificulten la identificación para el resto de personas.

La salida de documentos y soportes que contengan datos personales fuera de los locales que están bajo el control del responsable del tratamiento debe ser autorizada por este último. Este precepto también es aplicable a los documentos o soportes anexados y enviados por correo electrónico.

El inventario de documentos y soportes de OFTALMOS S.A. debe incluirse como anexo del presente manual.

4.1.2. Control de acceso

El personal de OFTALMOS S.A. solamente debe acceder a aquellos datos y recursos necesarios para el desarrollo de sus funciones y sobre los cuales se encuentren autorizados por el responsable del tratamiento en este manual.

OFTALMOS S.A. se ocupa del almacenamiento de una lista actualizada de usuarios, perfiles de usuarios, y de los accesos autorizados para cada uno de ellos. Además, tiene mecanismos para evitar el acceso a datos con derechos distintos de los autorizados. En el caso de soportes informáticos, puede consistir en la asignación de contraseñas, y en el caso de documentos, en la entrega de llaves o mecanismos de apertura de dispositivos de almacenamiento donde se archive la documentación.

La modificación sobre algún dato o información así como la concesión, alteración, inclusión o anulación de los accesos autorizados y de los usuarios recogidos en la lista actualizada mencionada en el párrafo anterior, corresponde de manera exclusiva al personal autorizado.

Cualquier personal ajeno a OFTALMOS S.A., que, de forma autorizada y legal, tenga acceso a los recursos protegidos, estará sometido a las mismas condiciones y tendrá las mismas obligaciones de seguridad que el personal propio.

Los usuarios autorizados para el acceso a las bases de datos se establecen en el numeral 6 de este manual.

4.1.3. Ejecución del tratamiento fuera de los locales

El almacenamiento de datos personales del responsable del tratamiento o encargado del tratamiento en dispositivos portátiles y su tratamiento fuera de los locales requiere una autorización previa por parte de OFTALMOS S.A., y el cumplimiento de las garantías de seguridad correspondientes al tratamiento de este tipo de datos.

4.1.4. Bases de datos temporales, copias y reproducciones

Las bases de datos temporales o copias de documentos creadas para trabajos temporales o auxiliares deben cumplir con el mismo nivel de seguridad que corresponde a las bases de datos o documentos originales. Una vez que dejan de ser necesarias, estas bases de datos temporales o copias son borradas o destruidas, impidiéndose así el acceso o recuperación de la información que contienen.

Solamente el personal autorizado en el numeral 6 puede realizar copias o reproducir los documentos.

4.1.5. Responsable de seguridad

OFTALMOS S.A., ha designado a doce responsables de seguridad encargados de coordinar y controlar las medidas de seguridad contenidas en el presente manual.

De acuerdo con la normativa sobre protección de datos, la designación de los responsables de seguridad no exonera de responsabilidad al responsable del tratamiento o encargado del tratamiento.

4.1.6. Auditorías

Las bases de datos que contengan datos personales, objeto de tratamiento por OFTALMOS S.A., clasificadas con nivel de seguridad sensible o privado, se han de someter, al menos cada dos años, a una auditoría interna o externa que verifique el cumplimiento de las medidas de seguridad contenidas en este manual.

Serán objeto de auditoría tanto los sistemas de información como las instalaciones de almacenamiento y tratamiento de datos.

OFTALMOS S.A., realizará una auditoría extraordinaria siempre que se realicen modificaciones sustanciales en el sistema de información que puedan afectar al cumplimiento de las medidas de seguridad, con el fin de verificar la adaptación, adecuación y eficacia de las mismas.

Las auditorías concluirán con un informe de auditoría que contendrá:

- El dictamen sobre la adecuación de las medidas y controles a la normativa sobre protección de datos.
- La identificación de las deficiencias halladas y la sugerencia de medidas correctoras o complementarias necesarias.
- La descripción de los datos, hechos y observaciones en que se basen los dictámenes y las recomendaciones propuestas.

El responsable de seguridad que corresponda estudiará el informe y trasladará las conclusiones al responsable del tratamiento para que implemente las medidas correctivas. Los informes de auditoría serán adjuntados al Manual Interno de Seguridad y quedarán a disposición de la Autoridad de Control.

4.2. Medidas de seguridad para bases de datos no automatizadas

4.2.1. Archivo de documentos

OFTALMOS S.A., fija los criterios y procedimientos de actuación que se deben utilizar para el archivo de documentos que contengan datos personales conforme a la Ley. Los criterios de archivo garantizan la conservación, localización y consulta de los documentos y hacen posible los derechos de consulta y reclamo de los Titulares. Estos criterios y procedimientos se recogen en el numeral 6 de este manual.

Se recomienda que los documentos sean archivados considerando, entre otros, criterios como el grado de utilización de los usuarios con acceso autorizado a los mismos, la actualidad de su gestión y/o tratamiento y la diferenciación entre bases de datos históricas y de administración o gestión de la empresa.

Los dispositivos de almacenamiento de documentos deben disponer de llaves u otros mecanismos que dificulte su apertura, excepto cuando las características físicas de éstos lo impidan, en cuyo caso OFTALMOS S.A., adoptará las medidas necesarias para impedir el acceso de personas no autorizadas.

Los dispositivos se identifican y describen en el numeral 6 del presente manual.

Cuando los documentos que contienen datos personales se encuentren en proceso de revisión o tramitación y, por tanto, fuera de los dispositivos de almacenamiento, ya sea antes o después de su archivo, la persona que se encuentre a cargo de los mismos debe custodiarlos e impedir en todo caso que personas no autorizadas puedan acceder a ellos.

Los dispositivos de almacenamiento que contengan documentos con datos personales clasificados con nivel de seguridad sensible deben encontrarse en áreas o locales en las que el acceso esté protegido con puertas de acceso con sistemas de apertura de llave u otros mecanismos similares. Estas áreas deben permanecer cerradas cuando no se precise el acceso a dichos documentos. Si no fuera posible cumplir con lo anterior, OFTALMOS S.A., podrá adoptar medidas alternativas debidamente motivadas que se incluirán en el presente manual.

La descripción de las medidas de seguridad de almacenamiento se encuentran recogidas en el numeral 6 de este documento.

4.2.2. Acceso a los documentos

El acceso a los documentos ha de realizarse exclusivamente por el personal autorizado en el numeral 6 del manual, siguiendo los mecanismos y procedimientos definidos. Estos últimos deben identificar y conservar los accesos realizados a la documentación clasificada con nivel de seguridad sensible, tanto por usuarios autorizados como por personas no autorizadas tal y como se refleja en el numeral referido anteriormente.

El procedimiento de acceso a los documentos que contienen datos clasificados como sensibles implica el registro de accesos a la documentación, la identidad de quien accede, el momento en que se produce el acceso y los documentos a los que se han accedido. El acceso a documentos con este tipo de datos se realiza por personal autorizado; si se realiza por personas no autorizadas deberá supervisarse por algún usuario autorizado o por el responsable de seguridad en cuestión de OFTALMOS S.A..

4.3. Medidas de seguridad para bases de datos automatizadas

4.3.1. Identificación y autenticación.

OFTALMOS S.A., debe instalar un sistema de seguridad informática que permita identificar y autenticar de forma correcta a los usuarios de los sistemas de información, con el fin de garantizar que solo el personal autorizado pueda acceder a las bases de datos.

También ha de establecer un mecanismo que permita la identificación personalizada e inequívoca de todo usuario que intente acceder al sistema de información y que verifique si está autorizado. La identificación debe realizarse mediante un sistema único para cada usuario que accede a la información teniendo en cuenta el nombre de usuario, la identificación de empleado, el nombre del departamento, etc. La nomenclatura utilizada para la asignación de nombres de usuario para acceder al sistema de información y el sistema de autenticación de los usuarios se recogen en el numeral 6 de este documento.

Cuando el sistema de autenticación esté basado en la introducción de contraseña, se ha de implantar un procedimiento de asignación, distribución y almacenamiento de

contraseñas; para garantizar la integridad y confidencialidad de estas últimas, se recomiendan que tengan un mínimo de nueve caracteres y contengan mayúsculas, minúsculas, números y letras. La política de contraseñas de OFTALMOS S.A., se encuentra en el numeral 6 del presente manual.

Por otra parte, OFTALMOS S.A., debe vigilar que las contraseñas se cambien de forma periódica, nunca por un tiempo superior a 365 días. El periodo de vigencia de las contraseñas se recoge en el ya referido numeral 6.

OFTALMOS S.A., también garantiza el almacenamiento automatizado, interno y cifrado, de las contraseñas mientras estén vigentes, y adoptará un mecanismo para limitar los intentos reiterados de accesos no autorizados, también detallado en el numeral 6 del manual.

4.3.2. Entrada y salida de documentos o soportes

La entrada de documentos o soportes debe registrarse indicando el tipo de documento o soporte, la fecha y hora, el emisor, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen según el nivel de seguridad, la forma de envío y la persona responsable de la recepción. La salida o envío de documentos o soportes, debidamente autorizada, ha de registrarse indicando el tipo de documento o soporte, la fecha y hora, el receptor, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen según el nivel de seguridad, la forma de envío y la persona responsable del envío.

El sistema de registro de entrada y salida debe ser anexado en el presente documento.

4.3.3. Control de acceso físico

Los locales que son sede de los sistemas de información que contienen datos personales deben estar debidamente protegidos con el fin de garantizar la integridad y confidencialidad de dichos datos; así mismo, han de cumplir con las medidas de seguridad físicas correspondientes al documento o soporte donde incluyen los datos.

OFTALMOS S.A., tiene el deber de poner en conocimiento de su personal las obligaciones que les competen con el objetivo de proteger físicamente los documentos o soportes en los que se encuentran las bases de datos, no permitiendo su manejo, utilización o identificación por personas no autorizadas en el presente manual. Los locales e instalaciones donde se ubican las bases de datos, especificando sus características físicas y las medidas de seguridad física existentes se señalan en el numeral 6 del presente documento.

Solamente el personal autorizado puede tener acceso a los lugares donde estén instalados los equipos que dan soporte a los sistemas de información, de acuerdo con lo dispuesto en numeral antes referido.

4.3.4. Copias de respaldo y recuperación de datos

OFTALMOS S.A., ha llevado a cabo los procedimientos de actuación necesarios para realizar copias de respaldo, al menos una vez a la semana, excepto cuando no se haya producido ninguna actualización de los datos durante ese periodo. Todas las bases de datos deben tener una copia de respaldo a partir de las cuales se puedan recuperar los datos.

De igual modo, ha establecido procedimientos para la recuperación de los datos con el objetivo de garantizar en todo momento la reconstrucción al estado en el que éstos se encontraban antes de su pérdida o destrucción. Cuando la pérdida o destrucción afecte a bases de datos parcialmente automatizadas se grabarán manualmente los datos dejando constancia de ello en este manual.

OFTALMOS S.A., se encargará de controlar el correcto funcionamiento y aplicación de los procedimientos de realización de copias de respaldo y recuperación de los datos cada 6 meses.

Los procedimientos de copia y respaldo se recogen en numeral 6 de este manual.

OFTALMOS S.A., debe conservar una copia de respaldo de los datos y de los procedimientos de recuperación de los mismos en un lugar distinto a aquel en el que se

encuentren los equipos donde se lleva a cabo su tratamiento. Este lugar deberá cumplir en todo caso las mismas medidas de seguridad exigidas para los datos originales.

4.3.5. Registro de acceso

De los intentos de acceso a los sistemas de información de OFTALMOS S.A., deberá guarda, como mínimo, la identificación del usuario, la fecha y hora en que se lleva a cabo, la base de datos a la que se accede, el tipo de acceso y si ese acceso ha sido autorizado o no autorizado. En caso de que el registro haya sido autorizado, se guarda la información que permita identificar el registro consultado.

Los responsables de seguridad de las bases de datos automatizadas se encargan de controlar los mecanismos que permiten el registro de acceso, revisar con carácter mensual la información de control registrada y elaborar un informe de las revisiones realizadas y los problemas detectados. Además, deben impedir la manipulación o desactivación de los mecanismos que permiten el registro de acceso.

Los datos que contiene el registro de acceso deben conservarse, al menos, durante dos años.

No será necesario el registro de acceso cuando el responsable del tratamiento sea una persona natural y garantice que solamente él tiene acceso y trata los datos personales. Estas circunstancias deben hacerse constar expresamente en el presente documento.

4.3.6. Redes de comunicaciones

El acceso a datos personales a través de redes de comunicaciones, públicas o privadas, debe someterse a medidas de seguridad equivalentes al acceso local de datos personales.

La transmisión de datos personales mediante redes públicas o inalámbricas de comunicaciones electrónicas se tiene que llevar a cabo cifrando dichos datos, o utilizando otro mecanismo similar que garantice que la información no sea inteligible ni manipulada por terceras personas.

5. Funciones y obligaciones del personal

Todas las personas que intervienen en el almacenamiento, tratamiento, consulta o cualquier otra actividad relacionada con los datos personales y sistemas de información de OFTALMOS S.A., deben actuar de conformidad a las funciones y obligaciones recogidas en el presente apartado.

OFTALMOS S.A., debe informar a su personal de servicio de las medidas y normas de seguridad que compete al desarrollo de sus funciones, así como de las consecuencias de su incumplimiento, mediante cualquier medio de comunicación que garantice su recepción o difusión (correo electrónico, tablón de anuncios, etc.). De igual modo, debe poner a disposición del personal el presente manual para que puedan conocer la normativa de seguridad de la empresa y sus obligaciones en esta materia en función del cargo que ocupan.

OFTALMOS S.A., cumple con el deber de información con su inclusión de acuerdos de confidencialidad y deber de secreto que suscriben, en su caso, los usuarios de sistemas de identificación referidos en el numeral 6 sobre bases de datos y sistemas de información, y mediante una circular informativa dirigida a los mismos.

Las funciones y obligaciones del personal de OFTALMOS S.A., se definen, con carácter general, según el tipo de actividad que desarrollan dentro de la empresa y, específicamente, por el contenido de este manual. La lista de usuarios y perfiles con acceso a los recursos protegidos están recogidos en el numeral 6 sobre bases de datos y sistemas de información. Con carácter general, cuando un usuario trate documentos o soportes que contiene datos personales tiene el deber de custodiarlos, así como de vigilar y controlar que personas no autorizadas no puedan tener acceso a ellos.

El incumplimiento de las obligaciones y medidas de seguridad establecidas en este manual por parte del personal al servicio de OFTALMOS S.A., es sancionable de acuerdo a la normativa aplicable a la relación jurídica existente entre el usuario y la empresa.

Las funciones y obligaciones de los usuarios de las bases de datos personales bajo responsabilidad de OFTALMOS S.A., son las siguientes:

- **Deber de secreto:** Aplica a todas las personas que, en el desarrollo de su profesión o trabajo, acceden a bases de datos personales y vincula tanto a usuarios como a prestadores de servicios contratados; en cumplimiento de este deber, los usuarios de la empresa u organización no pueden comunicar o relevar a terceras personas, datos que manejen o de los que tengan conocimiento en el desempeño o cargo de sus funciones, y deben velar por la confidencialidad e integridad de los mismos.

- **Funciones de control y autorizaciones delegadas**: El responsable del tratamiento puede delegar el tratamiento de datos a terceros, para que actúe como encargado del tratamiento, mediante un contrato de transmisión de datos. Cuando se firmen contratos de transmisión de datos, estos se anexarán en el presente manual (AnexoIV).

- **Obligaciones relacionadas con las medidas de seguridad implantadas:**

  - Acceder a las bases de datos solamente con la debida autorización y cuando sea necesario para el ejercicio de sus funciones.

  - No revelar información a terceras personas ni a usuarios no autorizados.

  - Observar las normas de seguridad y trabajar para mejorarlas.

  - No realizar acciones que supongan un peligro para la seguridad de la información.

  - No sacar información de las instalaciones de la organización sin la debida autorización.

- **Uso de recursos y materiales de trabajo:** Debe estar orientado al ejercicio de las funciones asignadas. No se autoriza el uso de estos recursos y materiales para fines personales o ajenos a las tareas correspondientes al puesto de trabajo. Cuando, por motivos justificados de trabajo, sea necesaria la salida de dispositivos periféricos o extraíbles, deberá comunicarse a los responsables de seguridad que podrán autorizarla y, en su caso, registrarla.

- **Uso de impresoras, escáneres y otros dispositivos de copia:** Cuando se utilicen este tipo de dispositivos debe procederse a la recogida inmediata de las copias, evitando dejar éstas en las bandejas de los mismos.

- **Obligación de notificar incidencias:** Los usuarios tienen la obligación de notificar las incidencias de las que tenga conocimiento a los responsables de seguridad, quienes se encargarán de su gestión y resolución. Algunos ejemplos de incidencias son: la caída del sistema de seguridad informática que permita el acceso a los datos personales a personas no autorizadas, el intento no autorizado de la salida de un documento o soporte, la pérdida de datos o la destrucción total o parcial de soportes, el cambio de ubicación física de bases de datos, el conocimiento por terceras personas de contraseñas, la modificación de datos por personal no autorizado, etc.

- **Deber de custodia de los soportes utilizados:** Obliga al usuario autorizado a vigilar y controlar que personas no autorizadas accedan a la información contenida en los soportes. Los soportes que contienen bases de datos deben identificar el tipo de información que contienen mediante un sistema de etiquetado y ser inventariados. Cuando la información esté clasificada con nivel de seguridad sensible el sistema de etiquetado solo debe ser comprensible para los usuarios autorizados a acceder a dicha información.

- **Responsabilidad sobre los terminales de trabajo y portátiles:** Cada usuario es responsable de su propio terminal de trabajo; cuando esté ausente de su puesto, debe bloquear dicho terminal (ej. protector de pantalla con contraseña) para impedir la visualización o el acceso a la información que contiene; y tiene el deber de apagar el terminal al finalizar la jornada laboral. Asimismo, los ordenadores portátiles han de estar controlados en todo momento para evitar su pérdida o sustracción.

- **Uso limitado de Internet y correo electrónico:** El envío de información por vía electrónica y el uso de Internet por parte del personal está limitado al desempeño de sus actividades en la empresa.

- **Salvaguarda y protección de contraseñas:** Las contraseñas proporcionadas a los usuarios son personales e intransferibles, por lo que se prohíbe su divulgación o comunicación a personas no autorizadas. Cuando el usuario accede por primera vez con la contraseña asignada es necesario que la cambie. Cuando sea necesario restaurar la contraseña, el usuario debe comunicarlo al administrador del sistema.

- **Copias de respaldo y recuperación de datos:** Debe realizarse copia de seguridad de toda la información de bases de datos personales de la empresa.

- **Deber de archivo y gestión de documentos y soportes:** Los documentos y soportes deben de ser debidamente archivados con las medidas de seguridad establecidas en el numeral 4 del presente manual.

6. Bases de datos y sistemas de información

Las bases de datos almacenadas y tratadas por OFTALMOS S.A., se recogen en la siguiente tabla (Tabla I), donde se indica el nivel de seguridad y el sistema de tratamiento de cada una de ellas.

Tabla I. Bases de datos y nivel de seguridad

Base de datos	Nivel de seguridad	Sistema de tratamiento
Pacientes - Digital	Alto	Informatico
Pacientes - fisico	Alto	Fisico
Proveedores - digital	Basico	Informatico
Proveedores - fisicos	Basico	Fisico
Empleados - digital	Alto	Informatico

Empleados - manual	Alto	Fisico
Convenios - Digital	Basico	Digital
Convenios - Manual	Basico	Manual
Juridica - Manual	Basico	Fisico
Accionistas - Manual	Basico	Fisico

La siguiente tabla (Tabla II) recoge la estructura de las bases de datos de OFTALMOS S.A..

Tabla II. Estructura de las Bases de datos Físicas

	Pacientes **físico**	Proveedores **físico**	**Empleados físico**	**Convenios físico**	**Juridica físico**	**Accionistas físico l**
Responsable del tratamiento	OFTALMOS S.A., nit: 860006626-8, dirección: AV Calle 100 N. 18A-51, teléfono: 2187077, correo electrónico: tusdatos@barraquer.com.co					
Encargado de consultas y reclamos	ARMANDO CRISTIAN REINEL CRETE identificado con cc: 11.342.003 de Zipaquirá, teléfono: 2187077, correo electrónico: tusdatos@barraquer.com.co					
Tipos de datos	Sensibles	Sensibles	Sensibles	Básico	Básico	Básico
Sistema de tratamiento	fisico					
Origen y procedencia de los datos	Recogidos por el responsable					
Colectivo o categoría de Titulares	Pacientes	Proveedores	Empleados y Ex empleados	Convenio	Procesos Juridicos	Accionestas

Tabla II.I Estructura de las Bases de datos digitales

	Pacientes Digital	Proveedores Digital	**Empleados** Digital	**Convenios** Digital
Responsable del tratamiento	OFTALMOS S.A., nit: 860006626-8, dirección: AV Calle 100 N. 18A-51, teléfono: 2187077, correo electrónico: tusdatos@barraquer.com.co			
Encargado de consultas y reclamos	ARMANDO CRISTIAN REINEL CRETE identificado con cc: 11.342.003 de Zipaquirá, teléfono: 2187077, correo electrónico: tusdatos@barraquer.com.co			
Tipos de datos	Sensibles	Sensibles	Sensibles	Básico
Sistema de tratamiento	Digital			
Origen y procedencia de los datos	Recogidos por el responsable			
Colectivo o categoría de Titulares	Pacientes	Proveedores	Empleados y Ex empleados	Convenios

OFTALMOS S.A. nombra a los siguiente responsables de seguridad y desarrolla medidas de seguridad específicas para cada base de datos. Todo ello se recoge en la siguiente tabla (Tabla III).

El nombramiento de los responsables de seguridad no exonera al responsable del tratamiento o encargado del tratamiento de sus obligaciones.

Tabla III. Responsables de seguridad y medidas de seguridad de las bases de datos fisicas

	Pacientes **físico**	**Empleados manual**	Proveedores **físico**	**Convenios Manual**	**Juridica manual**	**Accionistas manual**
Responsables de seguridad	MARCIA EMYTH SEDANO - Coordinadora	YURY MABY BERNAL FRANCO- Coordinadora de	(YURY MABY BERNAL FRANCO- Coordinadora de Recursos Humanos), (CARMEN MARITZA	ARMANDO CRISTIAN REINEL CRETE -	ARMANDO CRISTIAN REINEL CRETE -	ARMANDO CRISTIAN REINEL CRETE -

	Departamento Enfermeria	Recursos Humanos	RODRIGUEZ PEÑA- Coordinadora de Farmacia e Inventario),(ALEXANDER GIL DE LOS REYES- Ingeniero Biomédico),(MIRIAM CARVAJAL RODRIGUEZ- Jefe de Nutrición y servicios generales), (CLAUDIA JIMENA MORA ACOSTA- Coordinadora de Calidad y Atencion al Usuario), (MARYLIN STELLA CLAVIJO NARANJO- Directora Contable y Financiera), (PEDRO JOSE MURCIA CORTES- Coordinador de Facturacion y Tesoreria), (Rocio del Pilar Perez Sandoval - Directora de Tecnología y Sistemas), (MARIA DEL PILAR SALAMANCA FRANCO- Bacteriologa), (LUZ ADRIANA PEÑA URIBE- Coordinadora Dpto de Cirugía)	GERENTE GENERAL	GERENTE GENERAL	GERENTE GENERAL
Control de acceso físico	Usuarios autorizados, Doble llave		Usuarios autorizados, Llave			
Gestión documental	Archivo en carpetas AZ; almacenamiento en armarios; no se realiza transporte de documentos; destrucción de documentos mediante destructora de papel.					
Control de acceso lógico	Usuario y contraseña, registro de entradas, cambio de contraseñas una vez al año, bloqueo de acceso tras tres intentos					
Copias de	Copias de respaldo cada 30 días; procedimiento de recuperación					

respaldo y procedimiento de recuperación	
Sistema de identificación y autenticación	Usuario y contraseña, contraseña: longitud mínima: nueve caracteres, números y letras; cambio de contraseña al menos una vez al año, tres intentos de entrada, almacenamiento cifrado.
Registro de acceso a los documentos	Usuarios autorizados

Tabla III.I Responsables de seguridad y medidas de seguridad de las bases de datos fisicas

	Pacientes Digital	Proveedores Digital	**Empleados** Digital	**Convenios** Digital
Responsables de seguridad	Rocio del Pilar Perez Sandoval - Directora de Tecnología y Sistemas	Rocio del Pilar Perez Sandoval - Directora de Tecnología y Sistemas	YURY MABY BERNAL FRANCO- Coordinadora de Recursos Humanos	Rocio del Pilar Perez Sandoval - Directora de Tecnología y Sistemas
Control de acceso físico	Usuarios autorizados, Doble llave		Usuarios autorizados, Doble llave	Usuarios autorizados, Llave
Gestión documental	Archivo en carpetas AZ; almacenamiento en armarios; no se realiza transporte de documentos; destrucción de documentos mediante destructora de papel.			
Control de acceso lógico	Usuario y contraseña, registro de entradas, cambio de contraseñas una vez al año, bloqueo de acceso tras tres intentos			
Copias de respaldo y procedimiento de	Copias de respaldo cada 30 días; procedimiento de recuperación			

recuperación	
Sistema de identificación y autenticación	Usuario y contraseña, contraseña: longitud mínima: nueve caracteres, números y letras; cambio de contraseña al menos una vez al año, tres intentos de entrada, almacenamiento cifrado.
Registro de acceso a los documentos	Usuarios autorizados

OFTALMOS S.A. identifica en este manual, a los encargados del tratamiento así como las condiciones del encargo. Cuando exista contrato de transmisión de datos, los encargados del tratamiento se identifican en el anexo sobre transmisión de datos de este documento. Los encargados del tratamiento deberán cumplir con las funciones y obligaciones relacionadas con las medidas en materia de seguridad recogidas en el presente manual.

7. Procedimiento de notificación, gestión y respuesta ante incidencias

OFTALMOS S.A., establece un procedimiento de notificación, gestión y respuesta de incidencias con el fin de garantizar la confidencialidad, disponibilidad e integridad de la información contenida en las bases de datos que están bajo su responsabilidad.

Todos los usuarios y responsables de procedimientos, así como cualquier persona que tenga relación con el almacenamiento, tratamiento o consulta de las bases de datos recogidas en este documento, deben conocer el procedimiento para actuar en caso de incidencia.

El procedimiento de notificación, gestión y respuesta ante incidencias es el siguiente:

- Cuando una persona tenga conocimiento de una incidencia que afecte o pueda afectar la confidencialidad, disponibilidad e integridad de la información protegida de la empresa deberá comunicarlo, de manera inmediata, a los responsables de seguridad, describiendo detalladamente el tipo de incidencia producida, e indicando las personas que hayan podido tener relación con la

incidencia, la fecha y hora en que se ha producido, la persona que notifica la incidencia, la persona a quién se le comunica y los efectos que ha producido.

- Una vez comunicada la incidencia ha de solicitar al responsable de seguridad correspondiente un acuse de recibo en el que conste la notificación de la incidencia con todos los requisitos enumerados anteriormente.

OFTALMOS S.A., crea un registro de incidencias que debe contener: el tipo de incidencia, fecha y hora de la misma, persona que la notifica, persona a la que se le comunica, efectos de la incidencia y medidas correctoras cuando corresponda. Este registro es gestionado por el responsable de seguridad de la base de datos y debe incluirse como anexo en el presente manual. (Anexo III)

Asimismo, debe implementar los procedimientos para la recuperación de los datos, indicando quien ejecuta el proceso, los datos restaurados y, en su caso, los datos que han requerido ser grabados manualmente en el proceso de recuperación.

8. Medidas para el transporte, destrucción y reutilización de documentos y soportes

Cuando corresponda desechar cualquier documento (original, copia o reproducción) o soporte que contenga datos personales debe procederse a su destrucción o borrado, a través de la implementación de medidas orientadas a evitar el acceso o recuperación de la información contenida en dicho documento o soporte.

Antes de iniciar la destrucción se realizara un acata o se llevara el registro en un libro o agenda, en dicha a notación se describirá el documento objeto de destrucción, la fecha, hora y firma de las dos personas que evidencian la destrucción.

Cuando se lleve a cabo el traslado físico de documentos o soportes deben adoptar las medidas necesarias para impedir el acceso indebido, la manipulación, la sustracción o la pérdida de la información. El traslado de soportes que contengan datos personales se realiza cifrando la información, o utilizando cualquier otro mecanismo que garantice que no se manipule ni se acceda a la misma.

Los datos contenidos en dispositivos portátiles deben estar cifrados cuando se hallen fuera de las instalaciones que están bajo control de OFTALMOS S.A.. Cuando no sea posible el cifrado, se debe evitar el tratamiento de datos personales mediante este tipo de dispositivos; sin embargo, se podrá proceder al tratamiento cuando sea estrictamente necesario, adoptando para ello medidas de seguridad que tengan en cuenta los riesgos e incluyéndolas en el presente manual.

DISPOSICIÓN FINAL

El presente manual ha sido aprobado por OFTALMOS S.A., como responsable del tratamiento de datos, el 27-10-2016, aceptando su contenido, ordenando su ejecución y cumplimiento, con carácter general por todo el personal de la empresa, y en particular, por aquellos a los referidos en este documento.

+

_____

ARMANDO CRISTIAN REINEL CRETE

ANEXO I

SOLICITUDES DE ACCESO Y RECLAMOS POR LOS TITULARES

Tabla IV. Registro de solicitudes de acceso y de reclamos por parte de los Titulares

Identificación del usuario	
Nombre y apellidos del usuario	
Departamento	
Identificación del solicitante	
Tipo de procedimiento	
Fecha	
Tipo de solicitud	
Nombre y apellidos del solicitante	
C.C./NIT	
Dirección postal	
Municipalidad	
Observaciones	

ANEXO II

INVENTARIO DE DOCUMENTOS Y SOPORTES

Tabla V. Inventario de documentos y soportes		
Nombre	**Tipo de documento o soporte**	**Descripción**

ANEXO III

REGISTRO DE INCIDENCIAS

Tabla VI. Modelo de registro de incidencias

Fecha y hora	
Tipo de incidencia	
Descripción	
Efectos	
Medidas correctoras	
Emisor de la notificación	
Receptor de la notificación	
Persona que ejecuta el proceso de recuperación	
Datos restaurados	
Datos grabados manualmente	

ANEXO IV

TRANSMISIONES DE DATOS

OFTALMOS S.A., ha contratado los servicios de terceros que implican el acceso y/o tratamiento de datos de carácter personal de los que es responsable.

Tabla VII. Modelo de registro de transmisiones de datos

Particular o empresa con la que se contrata	
Identificación del contrato	**Condiciones del encargo**

ANEXO V

REGISTRO DE ENTRADA Y SALIDA DE DOCUMENTOS Y SOPORTES

Tabla VIII. Modelo de registro de entrada de documentos y soportes

Fecha y hora	
Tipo de documentos y/o soporte	
Número de documentos y/o soportes	
Tipo de información contenida	
Recepción	
Emisor	
Forma de envío	
Persona autorizada para la recepción	

Tabla IX. Modelo de registro de salida de documentos y soportes

Fecha y hora	
Tipo de documentos y/o soporte	
Número de documentos y/o soportes	
Tipo de información contenida	
Entrega	
Destinatario	
Forma de envío	
Persona autorizada para la entrega	