

FITNESS PEOPLE CENTRO MÉDICO DEPORTIVO S.A.S. INVERSIONES FITNESS S.A.S.	MANUAL MANUAL DE FUNCIONES, RESPONSABILIDADES Y PROCEDIMIENTOS DE PROTECCIÓN DE DATOS PERSONALES	Revisó: Coord. S.G.C.I. / Dir. Gestión Humana Aprobó: Gerencia General
Elaboró: Responsable de Protección de Datos Personales	Código: MN-GH-02 Revisión: 01	Pág. 1 de 17 Fecha: 02-09-26

MANUAL DE FUNCIONES, RESPONSABILIDADES Y PROCEDIMIENTOS

PROGRAMA INTEGRAL DE GESTIÓN DE DATOS PERSONALES (PIGDP)

FITNESS PEOPLE CENTRO MÉDICO DEPORTIVO S.A.S. · INVERSIONES FITNESS S.A.S.

Documento marco	PT-GH-02 Política de Tratamiento y Protección de Datos Personales (Rev. 02)
Fundamento	Ley 1581 de 2012 arts. 17 y 18; Decreto 1377 de 2013 arts. 23, 26 y 27 (responsabilidad demostrada); Guía SIC para la implementación del principio de responsabilidad demostrada; Guía SIC del Oficial de Protección de Datos Personales (2023).
Aplica a	Todos los cargos del Manual MN-GH-01, aprendices, practicantes, contratistas, proveedores y Encargados.
Encargado	Software Fitmevise
Responsable	Freddy Suarez Guayara -

CONTENIDO

FITNESS PEOPLE CENTRO MÉDICO DEPORTIVO S.A.S. INVERSIONES FITNESS S.A.S.	MANUAL MANUAL DE FUNCIONES, RESPONSABILIDADES Y PROCEDIMIENTOS DE PROTECCIÓN DE DATOS PERSONALES	Revisó: Coord. S.G.C.I. / Dir. Gestión Humana Aprobó: Gerencia General
Elaboró: Responsable de Protección de Datos Personales	Código: MN-GH-02 Revisión: 01	Pág. 2 de 17 Fecha: 02-09-26

1. OBJETIVO Y ALCANCE

Definir la estructura de gobierno, las funciones y responsabilidades de cada cargo y los procedimientos operativos mediante los cuales LA ORGANIZACIÓN implementa, mantiene, verifica y mejora el cumplimiento de la Política de Tratamiento y Protección de Datos Personales, de manera que pueda demostrar ante la Superintendencia de Industria y Comercio (SIC) la adopción de medidas apropiadas, efectivas y verificables (principio de responsabilidad demostrada).

Este Manual complementa el Manual de Funciones de Gestión Humana MN-GH-01: las funciones aquí descritas se entienden incorporadas al perfil de cada cargo y su cumplimiento hace parte de la evaluación de desempeño y del régimen disciplinario.

2. ESTRUCTURA DE GOBIERNO DE LA PROTECCIÓN DE DATOS

Nivel	Instancia	Rol principal
Estratégico	Gerencia General / Representante Legal	Aprueba la Política, asigna recursos, responde ante la SIC como Responsable del tratamiento.
Táctico	Comité de Protección de Datos Personales	Instancia colegiada de seguimiento: revisa riesgos, incidentes, indicadores y decide acciones de mejora. Sesiona trimestralmente.
Táctico	Responsable de Protección de Datos Personales (Oficial de Protección de Datos – OPD)	Lidera, coordina y verifica el Programa Integral de Gestión de Datos Personales; canal de atención de los Titulares y de la SIC.
Operativo	Directores, gerentes de sede, administradores, líderes y coordinadores	Responsables de las bases de datos de su proceso o sede ("dueños de la base de datos").
Operativo	Todos los trabajadores, aprendices, practicantes y contratistas	Usuarios de la información: aplican los controles y reportan incidentes.
Externo	Encargados del tratamiento (proveedores)	Tratan datos por cuenta de la organización bajo contrato de transmisión.

2.1 Comité de Protección de Datos Personales

Integrantes: Gerente General o su delegado (preside), Responsable de Protección de Datos (secretaría técnica), Director(a) de Gestión Humana, Director(a) Financiero(a) y Administrativo(a), Director(a) Asistencial y Deportiva (como custodio de historias clínicas), Director(a) de Marketing Digital, Director(a) Comercial, Líder de Control Interno / Auditoría Interna y el responsable de Sistemas o el proveedor tecnológico cuando se requiera. Funciones: aprobar el plan anual de trabajo del PIGDP; revisar el inventario de bases de datos y la matriz de riesgos; evaluar los incidentes de seguridad y las respuestas dadas; aprobar evaluaciones de impacto para nuevos tratamientos (biometría, cámaras, aplicaciones, campañas); hacer seguimiento a las consultas y reclamos; revisar los resultados de auditoría y decidir acciones correctivas. Se deja acta de cada sesión.

FITNESS PEOPLE CENTRO MÉDICO DEPORTIVO S.A.S. INVERSIONES FITNESS S.A.S.	MANUAL MANUAL DE FUNCIONES, RESPONSABILIDADES Y PROCEDIMIENTOS DE PROTECCIÓN DE DATOS PERSONALES	Revisó: Coord. S.G.C.I. / Dir. Gestión Humana Aprobó: Gerencia General
Elaboró: Responsable de Protección de Datos Personales	Código: MN-GH-02 Revisión: 01	Pág. 3 de 17 Fecha: 02-09-26

3. FUNCIONES Y RESPONSABILIDADES POR CARGO

3.1 Gerente General / Representante Legal

- Aprobar la Política de Tratamiento de Datos Personales, este Manual y sus actualizaciones, y garantizar su publicación.
- Designar formalmente al Responsable de Protección de Datos Personales y conformar el Comité de Protección de Datos.
- Asignar los recursos humanos, técnicos y financieros necesarios para el PIGDP (software, licencias, capacitación, asesoría jurídica, seguridad física).
- Firmar la inscripción y actualizaciones del RNBD, o delegar esta función por escrito.
- Representar a la organización ante la SIC en investigaciones administrativas y garantizar la respuesta oportuna a sus requerimientos.
- Aprobar los contratos con Encargados del tratamiento y las transferencias internacionales de datos.
- Incluir el cumplimiento de la protección de datos como criterio en la evaluación de desempeño de los directores.

3.2 Responsable de Protección de Datos Personales (Oficial de Protección de Datos – OPD)

Cargo que la ejerce	Coordinador del Sistema de Gestión de Calidad Integral (actualmente: Freddy Suárez Guayara). Puede reasignarse por decisión de Gerencia a la Dirección de Gestión Humana o a un profesional jurídico.
Perfil	Profesional en derecho, administración, ingeniería o áreas afines, con formación certificada en protección de datos personales (Ley 1581 de 2012), sistemas de gestión y seguridad de la información; conocimiento de la operación de la IPS y de los gimnasios; habilidades de comunicación, análisis y manejo confidencial de la información.
Dependencia	Reporta funcionalmente a la Gerencia General y administrativamente a la Dirección Administrativa / Gestión Humana. Actúa con independencia y no puede ser sancionado por el ejercicio de sus funciones.
Dedicación	Parcial, con un mínimo de 8 horas semanales dedicadas al PIGDP, ampliable durante auditorías, incidentes o requerimientos de la SIC.

Funciones (conforme a la Guía del Oficial de Protección de Datos de la SIC, 2023):

- Elaborar, actualizar y difundir la Política, el Aviso de Privacidad, este Manual, el Protocolo de datos sensibles y los formatos asociados; verificar al menos una vez al año su vigencia normativa.
- Mantener el inventario de bases de datos (Anexo 1) y la matriz de riesgos de privacidad; coordinar la evaluación de impacto antes de implementar nuevos tratamientos.
- Ser el canal oficial de atención de consultas, reclamos y revocatorias de los Titulares; llevar la matriz de solicitudes y garantizar el cumplimiento de los términos legales (10 y 15 días hábiles).
- Custodiar (o verificar la custodia de) las autorizaciones otorgadas por los Titulares y la evidencia de entrega del Aviso de Privacidad.

FITNESS PEOPLE CENTRO MÉDICO DEPORTIVO S.A.S. INVERSIONES FITNESS S.A.S.	MANUAL MANUAL DE FUNCIONES, RESPONSABILIDADES Y PROCEDIMIENTOS DE PROTECCIÓN DE DATOS PERSONALES	Revisó: Coord. S.G.C.I. / Dir. Gestión Humana Aprobó: Gerencia General
Elaboró: Responsable de Protección de Datos Personales	Código: MN-GH-02 Revisión: 01	Pág. 4 de 17 Fecha: 02-09-26

- Verificar anualmente, con Contabilidad, la obligación de inscripción en el RNBD; realizar la inscripción, la actualización anual, el reporte semestral de reclamos y el reporte de incidentes.
- Liderar la respuesta a incidentes de seguridad: contención, documentación, evaluación, notificación a Titulares, reporte a la SIC dentro de los 15 días hábiles y acciones correctivas.
- Diseñar y ejecutar el plan anual de capacitación en protección de datos (inducción y reinducción); conservar los registros de asistencia y evaluación.
- Revisar y aprobar, junto con el área jurídica, las cláusulas de autorización, confidencialidad y transmisión de datos en contratos laborales, de prestación de servicios, con proveedores, convenios corporativos y aliados.
- Mantener el registro de Encargados del tratamiento y verificar periódicamente su cumplimiento (cuestionario o auditoría).
- Coordinar la auditoría interna anual de cumplimiento y presentar sus resultados al Comité y a la Gerencia.
- Atender los requerimientos, visitas e investigaciones de la SIC y de otras autoridades, con el apoyo de Gerencia y del área jurídica.
- Asesorar a todas las áreas en el diseño de formatos, campañas, sistemas y procesos que involucren datos personales (privacidad desde el diseño y por defecto).
- Presentar al Comité un informe trimestral con los indicadores del numeral 6.

3.3 Director(a) de Gestión Humana y Auxiliar administrativo(a) y de Gestión Humana

- Recolectar los datos de aspirantes, trabajadores, aprendices y practicantes únicamente mediante los formatos institucionales que incluyen el Aviso de Privacidad y la autorización (inscripción de hoja de vida, consentimiento informado, solicitud de información HC, contrato).
- Verificar que todo contrato laboral, de aprendizaje o de práctica contenga las cláusulas de confidencialidad y de autorización de datos, y que el trabajador firme el Acuerdo de Confidencialidad F-GH-20 y la autorización específica de datos sensibles antes de iniciar labores.
- Custodiar las hojas de vida laborales en archivo bajo llave; mantener los exámenes médicos ocupacionales, incapacidades y la información de salud del SG-SST en carpeta separada de acceso restringido (solo Gestión Humana, responsable del SG-SST y médico laboral).
- Transferir a EPS, AFP, ARL, CCF, bancos y operadores de nómina únicamente los datos necesarios para la afiliación y el pago, por canales seguros.
- Incluir el módulo de protección de datos en la inducción corporativa y coordinar la reinducción anual con el OPD.
- Ejecutar el procedimiento de retiro (numeral 5.8): revocatoria de accesos, entrega de información, recordatorio de la obligación de confidencialidad.
- Depurar el banco de hojas de vida de aspirantes no seleccionados a los doce (12) meses.
- Tramitar en primera instancia las consultas y reclamos de trabajadores y aspirantes, con el OPD.

FITNESS PEOPLE CENTRO MÉDICO DEPORTIVO S.A.S. INVERSIONES FITNESS S.A.S.	MANUAL MANUAL DE FUNCIONES, RESPONSABILIDADES Y PROCEDIMIENTOS DE PROTECCIÓN DE DATOS PERSONALES	Revisó: Coord. S.G.C.I. / Dir. Gestión Humana Aprobó: Gerencia General
Elaboró: Responsable de Protección de Datos Personales	Código: MN-GH-02 Revisión: 01	Pág. 5 de 17 Fecha: 02-09-26

3.4 Director(a) Financiero(a) y Administrativo(a), Contador(a), Tesorería y Asistentes/Auxiliares contables

- Custodiar los datos tributarios, bancarios y de facturación de usuarios, trabajadores, contratistas y proveedores con acceso restringido.
- Informar al OPD, con el cierre anual de estados financieros, el valor de los activos totales de cada sociedad para determinar la obligación de inscripción en el RNBD.
- Verificar que los contratos con proveedores que traten datos (software, pasarelas, nube, mensajería, seguridad, exámenes ocupacionales) contengan la cláusula de transmisión de datos personales antes de la orden de compra o el primer pago.
- Conservar la información contable y de facturación por diez (10) años y coordinar su eliminación segura con acta.
- No compartir extractos, comprobantes ni datos bancarios de terceros por canales no institucionales.

3.5 Director(a) Comercial, Líderes comerciales (on line y corporativo), Gerentes de sede, Administradores(as) y Asesores(as) comerciales

- Recolectar los datos de usuarios y prospectos únicamente con el formulario de inscripción institucional (físico o digital) que incluye el Aviso de Privacidad y la autorización F-GH-19, y explicar al usuario, antes de firmar, que los datos de salud, biométricos e imagen son opcionales.
- Ofrecer siempre la alternativa no biométrica de ingreso (carné, QR, documento) y registrar en el sistema la opción elegida.
- No condicionar la venta del plan, la cortesía, el referido o la congelación a la entrega de datos sensibles ni a la autorización de comunicaciones comerciales.
- Registrar en el sistema/CRM el canal de contacto autorizado por el usuario y respetar los horarios y la frecuencia de la Ley 2300 de 2023 en el telemarketing, seguimiento de leads y cobranza.
- En convenios corporativos, tratar los datos de los trabajadores de la empresa aliada solo para validar el beneficio, bajo el acuerdo de transmisión o transferencia firmado con la empresa.
- Mantener la política de escritorio limpio en recepción: los formularios, PAR-Q y documentos de usuarios no permanecen a la vista; se archivan diariamente bajo llave y se entregan al archivo central según el procedimiento de la sede.
- No consultar ni compartir datos de usuarios (asistencia, planes, pagos, teléfono) con terceros —incluidos familiares o parejas del usuario— sin autorización escrita del Titular o requerimiento de autoridad.
- Recibir en la sede las consultas y reclamos de habeas data con el formato F-GH-21 y remitirlos el mismo día al OPD.
- Reportar de inmediato al OPD cualquier incidente (pérdida de formularios, acceso indebido al software, envío erróneo de información, hurto de equipos).

3.6 Director(a) Asistencial y Deportiva, Medicina del Deporte, Fisioterapeutas, Nutricionista, Psicóloga y personal de la IPS

- Obtener el consentimiento informado y la autorización de datos sensibles antes de la primera atención; informar el carácter facultativo y las consecuencias de no autorizar (imposibilidad de prestar el servicio de salud).

FITNESS PEOPLE CENTRO MÉDICO DEPORTIVO S.A.S. INVERSIONES FITNESS S.A.S.	MANUAL MANUAL DE FUNCIONES, RESPONSABILIDADES Y PROCEDIMIENTOS DE PROTECCIÓN DE DATOS PERSONALES	Revisó: Coord. S.G.C.I. / Dir. Gestión Humana Aprobó: Gerencia General
Elaboró: Responsable de Protección de Datos Personales	Código: MN-GH-02 Revisión: 01	Pág. 6 de 17 Fecha: 02-09-26

- Registrar la atención exclusivamente en la historia clínica institucional (física o electrónica), con usuario individual; nunca en dispositivos, chats o cuadernos personales.
- Garantizar la reserva de la historia clínica: solo la conoce el paciente, el equipo tratante, las autoridades en los casos legales y los terceros autorizados por escrito por el paciente. Las copias se entregan únicamente conforme al procedimiento del Comité de Historias Clínicas.
- No comentar diagnósticos ni condiciones de salud de usuarios con el personal comercial, deportivo o administrativo; a los entrenadores solo se comunican las restricciones o recomendaciones estrictamente necesarias para la seguridad del entrenamiento, con autorización del usuario.
- Custodiar los formatos PAR-Q, valoraciones y planes en archivo de acceso restringido; no dejarlos en las zonas de entrenamiento.
- Participar en el Comité de Historias Clínicas y aplicar los tiempos de retención de la Resolución 1995 de 1999.
- Presidir la respuesta a incidentes que afecten historias clínicas, junto con el OPD, e informar a la Secretaría de Salud cuando corresponda.

3.7 Líderes deportivos, Profesores de planta, grupales y personalizados

- Usar los datos de los usuarios (nombre, plan, restricciones de salud comunicadas) solo para prescribir y supervisar el entrenamiento.
- No tomar fotografías ni videos de usuarios para redes sociales personales ni institucionales sin la autorización de uso de imagen registrada por el área de marketing.
- No solicitar datos de contacto de los usuarios para fines personales ni contactarlos por canales no institucionales.
- Registrar la asistencia y las valoraciones únicamente en las herramientas institucionales.
- Los profesores personalizados con contrato de prestación de servicios firman el Acuerdo de Confidencialidad F-GH-20 y devuelven la información de sus usuarios al terminar el contrato.

3.8 Director(a) de Marketing Digital, Community Manager, Diseñador(a) gráfico(a), Audiovisual y Traffiker

- Publicar imágenes o testimonios de usuarios y trabajadores solo con la autorización de uso de imagen vigente (verificar en el registro antes de publicar); retirar el contenido dentro de los cinco (5) días hábiles siguientes a una revocatoria.
- No publicar imágenes de menores de edad sin autorización escrita del representante legal.
- Configurar las campañas de correo, SMS y WhatsApp solo con las bases de datos de usuarios que autorizaron comunicaciones comerciales; incluir en todo mensaje el mecanismo de exclusión y respetar los horarios de la Ley 2300 de 2023.
- Administrar el consentimiento de cookies del sitio web y de las landing pages; publicar y mantener actualizados en la web la Política y el Aviso de Privacidad.
- Verificar que las plataformas de marketing, CRM y pauta (Meta, Google, WhatsApp Business, etc.) tengan los términos de tratamiento de datos aceptados y registrarlas en el inventario de Encargados.
- Depurar las bases de leads y prospectos cada seis (6) meses.

FITNESS PEOPLE CENTRO MÉDICO DEPORTIVO S.A.S. INVERSIONES FITNESS S.A.S.	MANUAL MANUAL DE FUNCIONES, RESPONSABILIDADES Y PROCEDIMIENTOS DE PROTECCIÓN DE DATOS PERSONALES	Revisó: Coord. S.G.C.I. / Dir. Gestión Humana Aprobó: Gerencia General
Elaboró: Responsable de Protección de Datos Personales	Código: MN-GH-02 Revisión: 01	Pág. 7 de 17 Fecha: 02-09-26

- Reportar al OPD los incidentes en cuentas de redes sociales o plataformas (accesos no autorizados, suplantación, filtración de listas).

3.9 Responsable de Sistemas / proveedor de tecnología

- Crear, modificar y eliminar usuarios en el software de afiliados, historia clínica electrónica, nómina, CRM y correo únicamente con la solicitud formal del jefe del área y la matriz de perfiles aprobada; retirar accesos el mismo día del retiro del trabajador.
- Configurar contraseñas robustas, bloqueo por inactividad, doble factor donde exista, antivirus y actualizaciones en todos los equipos.
- Ejecutar y verificar las copias de respaldo; documentar las pruebas de restauración.
- Administrar los sistemas de videovigilancia y biometría: acceso restringido, bitácora de consultas y extracción de grabaciones, borrado automático a los 30 días.
- Mantener los registros de auditoría (logs) de acceso a historias clínicas y bases sensibles por un mínimo de un (1) año.
- Apoyar al OPD en la evaluación de impacto de nuevas herramientas y en la investigación técnica de incidentes.
- Ejecutar el borrado seguro de equipos y medios antes de su reasignación, venta o disposición final, con acta.

3.10 Líder de Control Interno / Auditoría Interna

- Incluir en el plan anual de auditoría la verificación del cumplimiento de la Política y de este Manual en todas las sedes (lista de chequeo del Anexo 3).
- Verificar por muestreo la existencia de autorizaciones firmadas, la política de escritorio limpio, el control de accesos y la atención de reclamos en término.
- Reportar los hallazgos al Comité de Protección de Datos y hacer seguimiento a los planes de mejora.

3.11 Coordinador y personal de mantenimiento, servicios generales, seguridad y logística

- No manipular ni leer documentos con datos personales que encuentren en oficinas, recepción o consultorios; entregarlos cerrados al administrador de la sede.
- Ejecutar la destrucción de documentos únicamente mediante triturado y bajo la instrucción del administrador o del OPD.
- El personal de seguridad y recepción registra a los visitantes en el formato institucional y no entrega información de usuarios o trabajadores a terceros.
- Custodiar las llaves de archivos y cuartos técnicos.

3.12 Todos los trabajadores, aprendices, practicantes y contratistas

- Conocer y cumplir la Política, este Manual y el Protocolo de datos sensibles; asistir a las capacitaciones.
- Firmar el Acuerdo de Confidencialidad F-GH-20 y mantener la reserva de la información incluso después del retiro.
- Usar credenciales personales e intransferibles; bloquear el equipo al ausentarse; no instalar software no autorizado.

FITNESS PEOPLE CENTRO MÉDICO DEPORTIVO S.A.S. INVERSIONES FITNESS S.A.S.	MANUAL MANUAL DE FUNCIONES, RESPONSABILIDADES Y PROCEDIMIENTOS DE PROTECCIÓN DE DATOS PERSONALES	Revisó: Coord. S.G.C.I. / Dir. Gestión Humana Aprobó: Gerencia General
Elaboró: Responsable de Protección de Datos Personales	Código: MN-GH-02 Revisión: 01	Pág. 8 de 17 Fecha: 02-09-26

- No copiar, fotografiar, enviar por WhatsApp o correo personal, ni almacenar en dispositivos personales o nubes no institucionales, bases de datos o documentos con datos personales.
- No divulgar datos de usuarios, pacientes, compañeros o proveedores, ni usarlos para fines personales o de terceros.
- Reportar de inmediato al jefe inmediato y al OPD cualquier incidente o sospecha de incidente.
- Orientar al Titular que desee ejercer sus derechos hacia los canales oficiales.

3.13 Encargados del tratamiento (proveedores externos)

Cumplir el contrato o cláusula de transmisión de datos (Anexo 3 de la Política PT-GH-02): tratar los datos solo para el objeto contratado, aplicar la Política, garantizar seguridad y confidencialidad, no subcontratar sin autorización, reportar incidentes en 48 horas, apoyar la atención de derechos en 3 días hábiles, permitir auditorías y devolver o suprimir los datos al terminar. El OPD mantiene el registro de Encargados (Anexo 2) y aplica el cuestionario de verificación al menos una vez al año.

4. MATRIZ DE RESPONSABILIDADES (RACI)

R = Responsable de ejecutar · A = Aprueba/rinde cuentas · C = Consultado · I = Informado

Convenciones: GG = Gerencia General · OPD = Oficial de Protección de Datos · GH = Gestión Humana · COM = Comercial y sedes · ASI = Asistencial · MKT = Marketing · SIS = Sistemas · CI = Control Interno

Actividad	GG	OPD	GH	COM	ASI	MKT	SIS	CI
Aprobar Política y Manual	A	R	C	I	C	I	C	I
Inventario de bases de datos	I	A/R	R	R	R	R	C	I
Recolección de autorizaciones	I	A	R	R	R	R	C	I
Atención consultas y reclamos	I	A/R	R	R	R	R	C	I
Gestión de incidentes	A	R	C	R	R	R	R	I
RNBD y reportes SIC	A	R	I	I	I	I	C	I
Contratos con Encargados	A	R	C	C	C	C	C	I
Capacitación	A	R	R	I	I	I	I	I
Control de accesos y seguridad TI	A	C	C	I	I	I	R	I
Videovigilancia y biometría	A	C	I	R	I	I	R	I
Uso de imagen y campañas	A	C	I	C	I	R	I	I
Auditoría de cumplimiento	A	C	I	I	I	I	I	R

FITNESS PEOPLE CENTRO MÉDICO DEPORTIVO S.A.S. INVERSIONES FITNESS S.A.S.	MANUAL MANUAL DE FUNCIONES, RESPONSABILIDADES Y PROCEDIMIENTOS DE PROTECCIÓN DE DATOS PERSONALES	Revisó: Coord. S.G.C.I. / Dir. Gestión Humana Aprobó: Gerencia General
Elaboró: Responsable de Protección de Datos Personales	Código: MN-GH-02 Revisión: 01	Pág. 9 de 17 Fecha: 02-09-26

5. PROCEDIMIENTOS OPERATIVOS

5.1 Inventario y clasificación de bases de datos

Objetivo: Identificar y documentar todas las bases de datos con datos personales.

N.º	Actividad	Responsable	Registro / término
1	Cada director o líder de proceso identifica las bases de datos físicas y digitales de su área y diligencia la ficha del Anexo 1 (nombre, finalidad, Titulares, tipos de datos, sensibles sí/no, soporte, ubicación, responsable, Encargados, medidas de seguridad, retención).	Directores / líderes	Anexo 1 — anual y ante cada nueva base
2	El OPD consolida el inventario, clasifica los datos (público, semiprivado, privado, sensible) y asigna el nivel de riesgo.	OPD	Inventario consolidado
3	El Comité revisa y aprueba el inventario; se usa como base para el RNBD.	Comité	Acta trimestral

5.2 Recolección de datos y obtención de la autorización

Objetivo: Garantizar que toda recolección sea informada y autorizada.

N.º	Actividad	Responsable	Registro / término
1	Antes de crear o modificar un formato, sistema, landing page o campaña que recolecte datos, el área solicita revisión al OPD (privacidad desde el diseño): datos mínimos necesarios, Aviso de Privacidad, autorización y casillas separadas para datos sensibles.	Área solicitante / OPD	Correo de aprobación — 5 días hábiles
2	Al momento de la recolección se entrega o exhibe el Aviso de Privacidad PT-GH-03 y se obtiene la autorización (firma, clic, grabación o conducta inequívoca documentada). Para menores, firma el representante legal.	Quien recolecta	F-GH-19 / formulario / registro digital
3	La autorización se archiva junto con el documento fuente (hoja de vida, contrato, ficha de inscripción, historia clínica) o en el módulo digital correspondiente.	Quien recolecta / archivo	Conservación: vigencia + 5 años
4	El sistema o carpeta registra la fecha de autorización, canal y finalidades específicas aceptadas (comercial, imagen, biometría, salud).	Administrador / Sistemas	Campo en software / CRM

5.3 Atención de consultas, reclamos y revocatorias

Objetivo: Responder en los términos de los artículos 14 y 15 de la Ley 1581 de 2012.

N.º	Actividad	Responsable	Registro / término
1	Recepción por cualquier canal; quien recibe diligencia el F-GH-21, lo radica y lo remite al OPD el mismo día.	Recepción / sede / web	F-GH-21 — mismo día

FITNESS PEOPLE CENTRO MÉDICO DEPORTIVO S.A.S. INVERSIONES FITNESS S.A.S.	MANUAL MANUAL DE FUNCIONES, RESPONSABILIDADES Y PROCEDIMIENTOS DE PROTECCIÓN DE DATOS PERSONALES	Revisó: Coord. S.G.C.I. / Dir. Gestión Humana Aprobó: Gerencia General
Elaboró: Responsable de Protección de Datos Personales	Código: MN-GH-02 Revisión: 01	Pág. 10 de 17 Fecha: 02-09-26

N.º	Actividad	Responsable	Registro / término
2	El OPD registra la solicitud en la matriz, verifica identidad y legitimación, y clasifica: consulta (10 días hábiles) o reclamo (15 días hábiles).	OPD	Matriz de solicitudes — 1 día hábil
3	Si el reclamo está incompleto, requiere al Titular dentro de los 5 días siguientes; si en 2 meses no subsana, se archiva por desistimiento.	OPD	Comunicación escrita
4	Inscribe la leyenda "RECLAMO EN TRÁMITE" en la base de datos (campo de observaciones del software o carpeta física) dentro de los 2 días hábiles.	Administrador / Sistemas	Registro en sistema
5	Solicita la información al dueño de la base de datos y a los Encargados (plazo interno 3 días hábiles); analiza y proyecta la respuesta con apoyo jurídico si se requiere.	OPD / dueño de la base	Correo interno
6	Si no es posible responder en término, informa al Titular los motivos y la nueva fecha (máximo 5 u 8 días hábiles adicionales).	OPD	Comunicación antes del vencimiento
7	Responde al Titular por el medio elegido, ejecuta la decisión en todas las bases (actualización, rectificación, supresión, revocatoria, exclusión comercial), retira la leyenda y archiva el expediente.	OPD / dueño de la base	Respuesta + constancia — 5 años
8	Reporta semestralmente al RNBD el número de reclamos por tipología (cuando aplique) y presenta el indicador al Comité.	OPD	Reporte RNBD

5.4 Gestión de incidentes de seguridad

Objetivo: Contener, documentar, notificar y corregir las violaciones a la seguridad de los datos.

N.º	Actividad	Responsable	Registro / término
1	Detección y reporte inmediato al jefe inmediato y al OPD (correo protecciondedatos@ / llamada). Se preserva la evidencia y no se manipulan equipos o documentos comprometidos.	Cualquier persona	Reporte — inmediato
2	Contención: bloqueo de credenciales, aislamiento de equipos, recuperación de documentos, cambio de contraseñas, aviso al proveedor.	OPD / Sistemas / Administrador	Hasta 24 horas
3	Registro en el formato de incidentes: descripción, fecha de detección, datos y Titulares afectados, bases de datos, causa probable, medidas.	OPD	Formato de incidentes — 48 horas
4	Evaluación del riesgo para los Titulares (probabilidad y gravedad; especial si hay datos sensibles o historias clínicas). Si el riesgo es alto, se notifica a los Titulares afectados con recomendaciones.	OPD / Comité (extraordinario)	Acta — 5 días hábiles
5	Reporte a la SIC a través del RNBD dentro de los 15 días hábiles siguientes a la detección; denuncia penal si hay delito (Ley 1273 de 2009); aviso a la Secretaría de Salud si afecta historias clínicas.	OPD / Gerencia	Constancia de reporte

FITNESS PEOPLE CENTRO MÉDICO DEPORTIVO S.A.S. INVERSIONES FITNESS S.A.S.	MANUAL MANUAL DE FUNCIONES, RESPONSABILIDADES Y PROCEDIMIENTOS DE PROTECCIÓN DE DATOS PERSONALES	Revisó: Coord. S.G.C.I. / Dir. Gestión Humana Aprobó: Gerencia General
Elaboró: Responsable de Protección de Datos Personales	Código: MN-GH-02 Revisión: 01	Pág. 11 de 17 Fecha: 02-09-26

N.º	Actividad	Responsable	Registro / término
6	Análisis de causa raíz, acciones correctivas, lecciones aprendidas y actualización de la matriz de riesgos; seguimiento en el siguiente Comité.	OPD / Comité	Plan de acción

5.5 Vinculación y verificación de Encargados del tratamiento

Objetivo: Asegurar que los terceros traten los datos con las garantías legales.

N.º	Actividad	Responsable	Registro / término
1	Antes de contratar un proveedor que acceda a datos (software, nube, pasarela, mensajería, seguridad, exámenes ocupacionales, temporal, contador externo), el área solicitante informa al OPD y diligencia el cuestionario de debida diligencia.	Área solicitante / OPD	Cuestionario Anexo 2
2	El OPD y el área jurídica verifican que el contrato incluya la cláusula de transmisión (Anexo 3 de la Política) y, si hay servidores en el exterior, el país de destino y las garantías.	OPD / Jurídica	Contrato firmado — antes del inicio
3	Se registra el Encargado en el inventario (Anexo 2) y en el RNBD cuando aplique.	OPD	Registro de Encargados
4	Verificación anual de cumplimiento (cuestionario, certificaciones, auditoría) y al finalizar el contrato, certificación de devolución o supresión de los datos.	OPD / área contratante	Informe anual / certificado

5.6 Control de accesos a sistemas e información

Objetivo: Aplicar el principio de mínimo privilegio.

N.º	Actividad	Responsable	Registro / término
1	Gestión Humana solicita a Sistemas la creación de usuarios con el perfil aprobado para el cargo (matriz de perfiles) el día del ingreso.	G. Humana / Sistemas	Solicitud de acceso
2	Se entrega al trabajador credencial individual; firma el compromiso de uso de credenciales y el Acuerdo de Confidencialidad.	Sistemas / G. Humana	F-GH-20
3	Los cambios de cargo o traslado de sede implican revisión del perfil; los accesos a historias clínicas y datos sensibles se limitan al personal asistencial y de SG-SST autorizado.	Jefe inmediato / Sistemas	Solicitud de cambio
4	Revisión semestral de usuarios activos vs. planta de personal; desactivación de usuarios sin uso o de personal retirado.	Sistemas / OPD	Acta de revisión

5.7 Capacitación y sensibilización

Objetivo: Asegurar que todo el personal conozca sus obligaciones.

FITNESS PEOPLE CENTRO MÉDICO DEPORTIVO S.A.S. INVERSIONES FITNESS S.A.S.	MANUAL MANUAL DE FUNCIONES, RESPONSABILIDADES Y PROCEDIMIENTOS DE PROTECCIÓN DE DATOS PERSONALES	Revisó: Coord. S.G.C.I. / Dir. Gestión Humana Aprobó: Gerencia General
Elaboró: Responsable de Protección de Datos Personales	Código: MN-GH-02 Revisión: 01	Pág. 12 de 17 Fecha: 02-09-26

N.º	Actividad	Responsable	Registro / término
1	Inducción: módulo de protección de datos (Política, Manual, Protocolo, Acuerdo de Confidencialidad, incidentes) antes de acceder a cualquier sistema.	G. Humana / OPD	Formato de inducción F-GH-03
2	Reinducción anual para todo el personal y capacitación específica para recepción/comercial (autorizaciones, biometría, Ley 2300), asistencial (historia clínica) y marketing (imagen, campañas).	OPD	Formato de capacitación + evaluación
3	Campañas de sensibilización (cartelera, correos, grupos institucionales) al menos dos veces al año.	OPD / Marketing	Evidencia de publicación

5.8 Retiro de trabajadores y terminación de contratos

Objetivo: Evitar fugas de información al finalizar el vínculo.

N.º	Actividad	Responsable	Registro / término
1	Gestión Humana informa a Sistemas la fecha de retiro; los accesos se desactivan ese mismo día (correo, software, CRM, cámaras, biométrico).	G. Humana / Sistemas	Formato entrega del cargo
2	El trabajador entrega los documentos, equipos, llaves y bases de datos a su cargo; se verifica que no conserve información en dispositivos personales.	Jefe inmediato	Paz y salvo de dependencias
3	Se le recuerda por escrito la vigencia indefinida de la obligación de confidencialidad (F-GH-20) y las consecuencias legales de su incumplimiento.	G. Humana	Constancia firmada

5.9 Conservación, supresión y disposición final

Objetivo: Aplicar la tabla de retención de la Política.

N.º	Actividad	Responsable	Registro / término
1	Cada dueño de base de datos revisa anualmente la información que cumplió su periodo de conservación.	Dueños de bases	Listado de depuración
2	El OPD valida que no exista obligación legal, reclamo en trámite o proceso judicial que impida la supresión.	OPD	Visto bueno
3	Supresión: borrado seguro en sistemas y copias, triturado de documentos físicos, con acta que indique fecha, base de datos, cantidad y responsables.	Sistemas / Administrador	Acta de supresión

5.10 Videovigilancia y biometría

Objetivo: Operar los sistemas conforme al numeral 19 de la Política.

FITNESS PEOPLE CENTRO MÉDICO DEPORTIVO S.A.S. INVERSIONES FITNESS S.A.S.	MANUAL MANUAL DE FUNCIONES, RESPONSABILIDADES Y PROCEDIMIENTOS DE PROTECCIÓN DE DATOS PERSONALES	Revisó: Coord. S.G.C.I. / Dir. Gestión Humana Aprobó: Gerencia General
Elaboró: Responsable de Protección de Datos Personales	Código: MN-GH-02 Revisión: 01	Pág. 13 de 17 Fecha: 02-09-26

N.º	Actividad	Responsable	Registro / término
1	Antes de instalar o reubicar cámaras o dispositivos biométricos, el administrador solicita al OPD la evaluación de impacto (ubicación, finalidad, señalización, retención, acceso).	Administrador / OPD	Evaluación aprobada
2	Se instalan los avisos de videovigilancia en accesos y áreas cubiertas; se verifica en la lista de chequeo mensual de la sede.	Administrador	Lista de chequeo
3	Las solicitudes de grabaciones (usuario, autoridad, SG-SST, disciplinario) se tramitan por escrito, se aprueban por el OPD o Gerencia y se registran en bitácora; las copias se custodian con acta.	Sistemas / OPD	Bitácora de grabaciones
4	Los usuarios y trabajadores que no autoricen biometría se registran con la alternativa; nunca se les niega el ingreso por esta razón.	Recepción	Registro en sistema

5.11 Atención de requerimientos de la SIC y otras autoridades

Objetivo: Responder de forma completa y oportuna.

N.º	Actividad	Responsable	Registro / término
1	Todo requerimiento se remite el mismo día de su recepción al OPD y a Gerencia; se registra la fecha límite.	Quien recibe	Registro de requerimientos
2	El OPD reparte los numerales entre las áreas competentes con plazos internos, consolida la respuesta con soportes y la revisa con el área jurídica.	OPD / áreas	Matriz de reparto
3	Gerencia firma y radica por la Sede Electrónica de la SIC antes del vencimiento; se archiva la constancia.	Gerencia / OPD	Constancia de radicación

6. INDICADORES DE SEGUIMIENTO

Indicador	Fórmula	Meta	Frecuencia
Oportunidad en consultas y reclamos	Solicitudes respondidas en término / total de solicitudes	100 %	Trimestral
Cobertura de autorizaciones	Usuarios y trabajadores con autorización archivada / total activos (muestreo)	≥ 98 %	Semestral
Capacitación	Personal capacitado en el año / total de personal	100 %	Anual
Incidentes	N.º de incidentes reportados y % gestionados en término	100 % gestionados	Trimestral
Encargados con contrato	Encargados con cláusula de transmisión / total de Encargados	100 %	Anual
Hallazgos de auditoría	Hallazgos cerrados / hallazgos abiertos	≥ 90 %	Anual
Accesos revisados	Usuarios revisados / usuarios activos	100 %	Semestral

FITNESS PEOPLE CENTRO MÉDICO DEPORTIVO S.A.S. INVERSIONES FITNESS S.A.S.	MANUAL MANUAL DE FUNCIONES, RESPONSABILIDADES Y PROCEDIMIENTOS DE PROTECCIÓN DE DATOS PERSONALES	Revisó: Coord. S.G.C.I. / Dir. Gestión Humana Aprobó: Gerencia General
Elaboró: Responsable de Protección de Datos Personales	Código: MN-GH-02 Revisión: 01	Pág. 14 de 17 Fecha: 02-09-26

7. VIGENCIA Y CONTROL DE CAMBIOS

Este Manual rige a partir de su aprobación y se revisa anualmente junto con la Política PT-GH-02. Rev. 01 (02-09-26): versión inicial.

ELABORÓ
FREDDY SUÁREZ GUAYARA
Responsable de Protección de Datos / Coord.
S.G.C.I.

REVISÓ
Nombre: _____
Director(a) de Gestión Humana

APROBÓ
Nombre: _____
Gerente General / Representante Legal

FITNESS PEOPLE CENTRO MÉDICO DEPORTIVO S.A.S. INVERSIONES FITNESS S.A.S.	MANUAL MANUAL DE FUNCIONES, RESPONSABILIDADES Y PROCEDIMIENTOS DE PROTECCIÓN DE DATOS PERSONALES	Revisó: Coord. S.G.C.I. / Dir. Gestión Humana Aprobó: Gerencia General
Elaboró: Responsable de Protección de Datos Personales	Código: MN-GH-02 Revisión: 01	Pág. 15 de 17 Fecha: 02-09-26

ANEXO 1 — FICHA DE INVENTARIO DE BASE DE DATOS

Nombre de la base de datos	
Sociedad responsable	Fitness People CMD S.A.S. () Inversiones Fitness S.A.S. ()
Proceso / área dueña	
Responsable (cargo)	
Finalidad(es)	
Titulares	Usuarios () Pacientes () Trabajadores () Aspirantes () Contratistas () Proveedores () Visitantes () Menores ()
Tipos de datos	Identificación () Contacto () Ubicación () Socioeconómicos () Financieros () Laborales () Educación () Salud () Biométricos () Imagen () Otros: _____
¿Contiene datos sensibles?	Sí () No () ¿De menores? Sí () No ()
Soporte y ubicación	Físico () — Sede/archivo: _____ Digital () — Sistema/servidor: _____ Nube () — Proveedor y país: _____
Forma de recolección y autorización	
Encargados / terceros con acceso	
Transferencias (nacionales / internacionales)	
Medidas de seguridad	
N.º aproximado de Titulares	
Periodo de conservación	
Fecha de creación / última actualización	

FITNESS PEOPLE CENTRO MÉDICO DEPORTIVO S.A.S. INVERSIONES FITNESS S.A.S.	MANUAL MANUAL DE FUNCIONES, RESPONSABILIDADES Y PROCEDIMIENTOS DE PROTECCIÓN DE DATOS PERSONALES	Revisó: Coord. S.G.C.I. / Dir. Gestión Humana Aprobó: Gerencia General
Elaboró: Responsable de Protección de Datos Personales	Código: MN-GH-02 Revisión: 01	Pág. 16 de 17 Fecha: 02-09-26

ANEXO 2 — REGISTRO Y CUESTIONARIO DE ENCARGADOS DEL TRATAMIENTO

Encargado	Servicio	Bases de datos / tipos de datos	País de los servidores	Contrato con cláusula de transmisión (fecha)	Última verificación

Cuestionario de debida diligencia (respuesta Sí / No / Evidencia): 1. ¿Cuenta con política de tratamiento de datos publicada? 2. ¿Está inscrito en el RNBD (si aplica)? 3. ¿Dónde se almacenan los datos y quién accede a ellos? 4. ¿Cifra la información en tránsito y en reposo? 5. ¿Realiza copias de respaldo y pruebas de restauración? 6. ¿Su personal firma acuerdos de confidencialidad? 7. ¿Subcontrata parte del servicio? ¿Con quién? 8. ¿Tiene procedimiento de gestión de incidentes y plazo de notificación al cliente? 9. ¿Cómo apoya la atención de derechos de los Titulares? 10. ¿Devuelve o suprime los datos al terminar el contrato y certifica la supresión? 11. ¿Cuenta con certificaciones (ISO 27001 u otras)? 12. ¿Ha sido sancionado por la SIC en los últimos 5 años?

FITNESS PEOPLE CENTRO MÉDICO DEPORTIVO S.A.S. INVERSIONES FITNESS S.A.S.	MANUAL MANUAL DE FUNCIONES, RESPONSABILIDADES Y PROCEDIMIENTOS DE PROTECCIÓN DE DATOS PERSONALES	Revisó: Coord. S.G.C.I. / Dir. Gestión Humana Aprobó: Gerencia General
Elaboró: Responsable de Protección de Datos Personales	Código: MN-GH-02 Revisión: 01	Pág. 17 de 17 Fecha: 02-09-26

ANEXO 3 — LISTA DE CHEQUEO DE CUMPLIMIENTO POR SEDE

N.º	Ítem de verificación	Cumple	No cumple	Observación
1	Aviso de Privacidad visible en recepción y en los formularios de inscripción.			
2	Formularios de inscripción incluyen autorización F-GH-19 con casillas separadas para salud, biometría, imagen y comunicaciones comerciales.			
3	Muestra de 10 usuarios activos: autorización firmada y archivada.			
4	Se ofrece y funciona la alternativa no biométrica de ingreso.			
5	Avisos de videovigilancia instalados en accesos y áreas cubiertas; sin cámaras en vestidores, baños, duchas ni consultorios.			
6	Escritorio limpio: no hay formularios, PAR-Q ni documentos de usuarios a la vista; archivo bajo llave.			
7	Historias clínicas y datos de salud en archivo de acceso restringido; copias solo por procedimiento.			
8	Equipos con bloqueo por inactividad y usuarios individuales; no hay contraseñas compartidas o anotadas.			
9	Personal de la sede capacitado en el último año (registro).			
10	Trabajadores y contratistas de la sede con Acuerdo de Confidencialidad firmado.			
11	Formato F-GH-21 disponible y el personal conoce el canal de reclamos y los términos.			
12	Documentos con datos personales se destruyen mediante triturado; existe acta.			
13	Publicaciones en redes de la sede con autorización de uso de imagen verificable.			
14	Contactos comerciales y de cobranza dentro de los horarios de la Ley 2300 de 2023.			
15	Incidentes del periodo reportados al OPD.			

Sede: _____ Fecha: ____ / ____ / ____ Auditor: _____
Administrador(a): _____