Manual Interno de Seguridad de la Información
Tratamiento de Datos Personales
Club Miramar

1. Introducción

El Club Miramar, comprometido con la protección de los datos personales de sus socios, empleados, contratistas, proveedores y visitantes, adopta el presente Manual Interno de Seguridad de la Información como complemento a sus políticas de protección de datos personales adoptadas en el año 2018.
Este manual contiene las directrices, responsabilidades y procedimientos orientados a prevenir la adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento de los datos personales almacenados en servidores propios del Club.

2. Marco Normativo

Este manual se fundamenta en la Ley 1581 de 2012, el Decreto 1377 de 2013, las decisiones administrativas de la Superintendencia de Industria y Comercio, y los pronunciamientos de la Corte Constitucional, en especial las sentencias SU-082 de 1995, T-580 de 1995, T-448 de 2004, T-526 de 2004, T-657 de 2005, T-684 de 2006, C-1011 de 2008 y T-017 de 2011.
Los principios de legalidad y libertad son pilares fundamentales: ningún dato podrá ser tratado sin el consentimiento previo, expreso e informado del titular, ni podrá ser transferido para fines distintos a los autorizados.

3. Principios Rectores del Tratamiento de Datos Personales

3.1. Principio de Legalidad en el Tratamiento

El tratamiento de datos personales en el Club solo se realiza cuando[1]:

[1] Según el artículo 4 de la Ley 1581 de 2012 y la Sentencia SU-082 de 1995. El tratamiento de datos personales será realizado por disposición de la ley.

(i) Exista autorización previa, expresa e informada del titular;

(ii) O exista una disposición legal que lo habilite (ej. datos laborales o contractuales).
Toda actividad de recolección, almacenamiento, consulta, uso o supresión de datos personales será realizada bajo parámetros estrictamente normativos y registrados en los procedimientos internos.

3.2. Principio de Finalidad Específica y Legítima

Los datos personales se recolectan exclusivamente para fines relacionados con[2] :

i. Gestión administrativa de socios;
ii. Administración de reservas, torneos, escuelas deportivas y servicios de hotelería;
iii. Gestión del talento humano y cumplimiento legal. Está prohibido el uso posterior de los datos para fines distintos, salvo que el titular otorgue una nueva autorización, según lo exige el principio de autodeterminación informática.

3.3. Principio de Libertad del Titular para Autorizar

El Club recolecta datos solo con la autorización expresa del titular, mediante formatos físicos o electrónicos[3].

i. El consentimiento es libre y puede ser revocado en cualquier momento, respetando el derecho a la autodeterminación.

3.4. Principio de Veracidad o Calidad de los Datos

El Club mantiene mecanismos de verificación y actualización periódica de

[2] La Ley exige que los datos se recolecten con fines claros, explícitos y legítimos. Así lo ratifica la Sentencia T-017 de 2011.

[3] El consentimiento del titular es el eje central del habeas data, según la Corte Constitucional. No puede condicionarse el acceso a servicios al suministro de datos innecesarios (SU-082/95, T-684/06).

la información[4].

i. Los titulares tienen derecho a solicitar en cualquier momento la corrección o actualización de sus datos, a través de canales claramente establecidos en la política.

3.5. Principio de Seguridad y Confidencialidad: Se ha adoptado un Manual Interno de Seguridad de la Información[5], que detalla las medidas técnicas y organizativas aplicadas en los servidores propios.

i. El acceso a la información está restringido por roles.

ii. Se implementan mecanismos de cifrado, autenticación, respaldo periódico y control de incidentes.

iii. Terceros que accedan a la información deben firmar acuerdos de confidencialidad.

3.6. Principio de Acceso y Circulación Restringida

Los datos personales almacenados por el Club no pueden ser divulgados a entidades externas ni ser transferidos sin autorización previa del titular[6].

[4] Solo pueden tratarse datos que sean completos, veraces y actualizados. La inexactitud puede vulnerar el buen nombre (Sentencias SU-082/95 y T-448/04).

[5] Establecido por el artículo 19 de la Ley 1581 de 2012 y reforzado por decisiones administrativas de la SIC.

[6] Solo personas autorizadas pueden acceder a los datos. No se permite su divulgación a terceros sin consentimiento (T-580/95 y C-1011/08).

Cualquier solicitud de información por parte de un tercero debe pasar por un proceso de análisis jurídico, acompañado de:

i. Solicitud formal de acceso,
ii. Autorización del titular,
iii. Y compromiso de uso bajo confidencialidad.

4. Desarrollo de Medidas de Seguridad en Servidores Propios

Se establecen los lineamientos bajo los cuales se diseñan, implementan y controlan las medidas técnicas, físicas y administrativas necesarias para garantizar la protección de los datos personales. Dichas medidas, ajustadas al marco normativo vigente, responden a una operación basada en infraestructura tecnológica propia, lo que implica asumir de manera directa la responsabilidad sobre la seguridad en el tratamiento de la información.

4.1. Restricción de accesos a servidores y bases de datos.

i. Creación de roles y perfiles con privilegios mínimos.
ii. Control de acceso físico con llave, tarjeta o registro manual.
iii. Gestión de usuarios autorizados y monitoreo de sesiones activas.

4.2. Políticas de contraseñas seguras y doble autenticación.

i. Contraseñas con mínimo 12 caracteres, incluyendo símbolos y números.
ii. Renovación obligatoria cada 90 días.
iii. Activación de doble autenticación (2FA) mediante app o token físico.

4.3. Cifrado de información sensible.

i. Cifrado de disco completo en servidores físicos (BitLocker, LUKS).
ii. Protección con contraseña de archivos sensibles (Word, PDF, Excel).
iii. Implementación de HTTPS en interfaces web internas.

4.4. Registros de logs y monitoreo de accesos.

i. Activación de logs en bases de datos y sistemas operativos.
ii. Revisión quincenal de logs para identificar accesos irregulares.
iii. Conservación mínima de 6 meses de registros de acceso.

4.5. Respaldos periódicos en servidores controlados.

i. Programación de copias de seguridad automáticas diarias o semanales.

ii. Almacenamiento en discos duros cifrados o ubicaciones segmentadas.
iii. Pruebas de restauración trimestrales para verificar la integridad del respaldo.

4.6. Procedimientos para gestión de incidentes y filtraciones.

i. Definición de protocolos internos frente a pérdida, fuga o alteración de datos.
ii. Asignación de responsables técnicos y jurídicos ante cada tipo de incidente.
iii. Registro en bitácora y análisis de causas y medidas correctivas.

5. Procedimientos Internos para el Tratamiento de Datos Personales

las directrices de la Superintendencia de Industria y Comercio (SIC), en el marco del tratamiento de datos personales en servidores propios.

5.1 Creación, Modificación y Eliminación Segura de Registros

Garantizar que cualquier incorporación o alteración de datos personales en las bases del Club se haga bajo condiciones controladas, auditables y seguras.

5.1.2 Procedimiento:

i. Solo personal autorizado podrá crear o modificar registros. Toda modificación debe quedar registrada (fecha, usuario, motivo).
ii. Se deben utilizar formularios o sistemas que validen la integridad del dato (campos obligatorios, formatos estandarizados).
iii. La eliminación debe ejecutarse solo si:
   - El titular lo solicita.
   - La finalidad del tratamiento se ha agotado.
   - Han vencido los plazos legales o contractuales.
iv. En caso de eliminación, se debe hacer de forma irrecuperable, usando herramientas de sobreescritura segura o borrado físico (según el medio).

Nota: Soporte documental requerido:
1. Bitácoras de creación/modificación.
2. Formatos de solicitud de supresión o corrección.

5.2. Verificación del Consentimiento antes de Cualquier Tratamiento

Hay que asegurar que ningún dato personal sea tratado sin el consentimiento válido, expreso e informado del titular, salvo que exista una base legal habilitante.

Procedimiento:

i. Verificar existencia de autorización escrita o evidencia electrónica con trazabilidad.
ii. Conservar copia digital o física de la autorización.
iii. Registrar la fecha y medio del consentimiento en los sistemas.

Medios válidos:
- Formularios físicos firmados:
- Checkboxes digitales con IP y timestamp.
- Correos electrónicos con declaración expresa del titular.

5.2.1. Anexo Procedimiento Específico de Consentimiento Informado y Autorizaciones

Aplica de manera transversal a todos los escenarios en los que el Club recolecta o trata datos personales, ya sea de socios, usuarios, empleados, contratistas, proveedores o visitantes.

- Escenarios Cubiertos

i. Formularios de inscripción y permanencia en escuelas deportivas ya sean adultos o menores de edad.
ii. Registro y consentimiento de uso de imagen a través de cámaras de seguridad.
iii. Registro y autorizaciones en procesos de alojamiento y reservas en el hotel.
iv. Contratación de personal, manejo de hojas de vida y expedientes laborales.
v. Relación con proveedores y contratistas (contratos, pagos, facturación).

6.Procedimiento Operativo

i. Verificar existencia de autorización escrita o evidencia electrónica con trazabilidad, antes de cualquier tratamiento de datos personales.

ii. Conservar copia digital o física del consentimiento otorgado por el titular. Este soporte debe estar disponible en caso de auditoría o ejercicio de derechos por parte del titular.

iii. Registrar en los sistemas institucionales la fecha, medio y finalidad específica para la cual se otorgó el consentimiento.

6.1. Medios Válidos para Recoger el Consentimiento

i. Formularios físicos firmados por el titular o su representante legal (en caso de menores).
ii. Checkboxes digitales con validación de IP, hora y trazabilidad, dentro de plataformas o formularios web.

iii. Correos electrónicos en los que el titular manifieste su autorización expresa con fines determinados.

6.2. Tratamiento de Datos Personales de Niños, Niñas y Adolescentes

Como parte de su labor educativa, recreativa y formativa, se reconoce que algunos datos personales de niños, niñas y adolescentes pueden requerir tratamiento. Dado su carácter excepcional, este solo se realiza cuando es estrictamente necesario y con el único propósito de garantizar su bienestar, seguridad y participación adecuada en las actividades ofrecidas.

Ciertos datos sensibles —como información médica básica, condiciones físicas o imágenes en contexto institucional— podrán ser tratados exclusivamente para:

- Brindar atención oportuna en caso de emergencia.
- Realizar seguimientos deportivos, académicos o de convivencia.
- Implementar medidas de protección y acompañamiento individualizado.

6.2.1. Procedimiento para el Tratamiento de Datos de Niños, Niñas y Adolescentes

El tratamiento de datos personales de menores de edad se realiza únicamente cuando es estrictamente necesario y bajo condiciones reforzadas de protección. En estos casos, se aplica el siguiente procedimiento:

i. **Autorización del representante legal:**

   El consentimiento debe ser otorgado por el padre, madre o acudiente del menor, mediante un formulario físico o digital. Esta autorización debe conservarse con carácter obligatorio y estar disponible para efectos de trazabilidad y verificación.

ii. **Finalidad clara y proporcional:**

   Toda autorización debe incluir información comprensible sobre la finalidad del tratamiento, el tiempo durante el cual se conservarán los datos y los derechos del titular o su representante.

iii. **Medidas especiales de seguridad:**

   Los datos se tratan bajo condiciones reforzadas de confidencialidad, con acceso restringido, medidas de seguridad técnica y control administrativo diferenciado.

iv. **Principio de necesidad:**

   La recolección se limita únicamente a la información esencial para garantizar el bienestar, participación y cuidado del menor en las actividades ofrecidas.

v. **Revocatoria del consentimiento:**

   El consentimiento podrá ser revocado en cualquier momento mediante solicitud escrita o digital. En ese caso, se activarán los mecanismos internos para detener el tratamiento y, de ser procedente, eliminar la información de forma segura.

6.3 Revisión Periódica del Acceso a Datos

Objetivo: Garantizar que el acceso a las bases de datos personales esté restringido exclusivamente a personal autorizado, con control y trazabilidad.

Procedimiento:

i. Revisión trimestral de:
- Usuarios activos en bases de datos.
- Roles asignados.
- Logs de acceso.

ii. Revocación de accesos a personas retiradas o que cambian de funciones.
iii. Cierre inmediato de accesos injustificados.

Instrumentos de control:
- Listado de usuarios y permisos.
- Logs del sistema.
- Formato de auditoría interna.

6.4. Eliminación Segura y Definitiva de Datos Caducos

Objetivo: Evitar la retención innecesaria o riesgosa de datos personales que ya no tienen justificación legal o contractual.

6.4.1 Procedimiento:

i. Revisión semestral del inventario de datos.
ii. Identificación de registros que han cumplido su finalidad o plazos legales.
iii. Aplicación de:
- Eliminación lógica
- Eliminación física (triturado, sobreescritura, incineración).
- Registro detallado del proceso de depuración.

Ejemplo de plazos de conservación:

- Registros contables: 10 años.
- Hoja de vida: 2 años tras finalización del vínculo.
- Datos de reservas: hasta 6 meses después del servicio.

Evidencia requerida:
- Informe de depuración de bases.
- Acta de destrucción.

7. Responsables en Materia de Protección de Datos

Se identifica los responsables claves para la gestión integral del programa de protección de datos personales, por parte de la circular única y recomendaciones de la Superintendencia de Industria y Comercio (SIC).

7.1. Administrador de Sistemas

Rol: Responsable técnico de la infraestructura tecnológica que soporta el tratamiento de datos personales.

Funciones:
- Gestionar accesos a los servidores, redes y bases de datos del Club.
- Implementar y supervisar controles de seguridad (cifrado, respaldo, autenticación).
- Generar y custodiar los logs de acceso y actividad.
- Apoyar al Oficial de Protección de Datos (OPD) en la gestión de incidentes de seguridad.
- Colaborar en evaluaciones de impacto sobre privacidad desde el diseño.

Recomendación SIC: Asegurar el acompañamiento del área tecnológica en todas las fases del ciclo de vida de los datos, especialmente en proyectos de nuevos sistemas o actualizaciones.

7.2. Oficial de Protección de Datos (OPD)

Rol: Persona o área encargada de velar por el cumplimiento del Régimen General de Protección de Datos Personales dentro del Club.

Funciones recomendadas por la SIC:
- Supervisar la implementación y cumplimiento de la política de datos.
- Actuar como punto de contacto entre el Club, los titulares de la información y la SIC.
- Presidir o participar en el comité de protección de datos del Club.
- Coordinar la elaboración y actualización del Registro Nacional de Bases de Datos.
- Asesorar en evaluaciones de impacto, auditorías, análisis de riesgo y capacitación.
- Emitir recomendaciones documentadas ante incidentes o decisiones de alto impacto.
- Contar con autonomía, recursos y formación continua.

- Rendir cuentas ante la alta dirección del Club.

Buenas prácticas:
- Publicar su contacto institucional.
- Garantizar su independencia y evitar conflictos de interés.
- Participar desde el diseño de cualquier proyecto que involucre tratamiento de datos ("privacy by design"). Que es lo que se trata este diseño.

7.3. Dirección Administrativa

Rol: Responsable del control institucional de las políticas internas del Club y autoridad para adoptar, modificar o aprobar los lineamientos y procedimientos.

Funciones clave:
- Emitir decisiones directivas que aprueben políticas y manuales de protección de datos.
- Aprobar los recursos humanos y técnicos para implementar el programa de gestión de datos.
- Supervisar la ejecución de los planes de formación, seguimiento y auditoría interna.
- Apoyar la trazabilidad documental de las decisiones que involucran tratamiento de datos personales.
- Garantizar la rendición de cuentas del OPD ante el nivel directivo.

Recomendación SIC: La alta dirección debe integrar la protección de datos como tema estratégico, apoyando su gobernanza interna y asumiendo responsabilidad activa frente a la SIC en caso de incumplimiento.