POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

HISTÓRICO DE VERSIONES		
Versión	**Fecha**	**Resumen de los cambios producidos**
1	25-1-2026	Primera versión aprobada.

Elaborado:	Aprobado:
Responsable de seguridad **TOMAS RAMOS SUAREZ**	Director Gerente **FRANCISCO JAVIER PESCADOR PEREZ**

Contenido

1 – APROBACIÓN Y ENTRADA EN VIGOR

El presente documento contiene la Política de Seguridad de la Información de **SPORT STUDIO SERVICIOS DEPORTIVOS SL**, (en adelante, "La Política" y "La organización"). Esta Política ha sido aprobada por la empresa el 25-1-2026, fecha en la que entra en vigor, e implica la derogación de cualquier otra existente hasta la fecha y se mantendrá vigente hasta que sea sustituida por una nueva Política.

La organización pondrá a disposición de interesados legítimos a través de su página *web* la versión actualizada del documento de Política de Seguridad de la Información.

2 – INTRODUCCIÓN

El presente documento tiene por objeto establecer la política de seguridad de la información en base a los requisitos dispuestos por el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (en adelante ENS), garantizando la seguridad de la información y, por supuesto, garantizando el cumplimiento de todas las obligaciones legales, contractuales y reglamentarias aplicables en el marco de la seguridad de la información y de la protección de los datos personales.

La política de seguridad de la organización tiene por objetivo marcar las pautas de alto nivel a seguir para que todos los tratamientos de información relativos a los procesos de negocio indicados en el alcance se realicen de forma segura y únicamente por personal autorizado, así como proteger la información de la organización ante posibles pérdidas de confidencialidad, integridad y/o disponibilidad, o afecciones a la trazabilidad o la autenticidad.

El Comité de Seguridad de la Información garantizará la difusión de la Política, la compresión e implicación de todo el personal en el logro de los objetivos.

3 – OBJETIVOS Y MISIÓN DE LA ORGANIZACIÓN

Sport Studio Servicios Deportivos es una sociedad limitada cuyo objeto social fundamental es:

"Nuestra vocación deportiva nos hace pensar que en Sport Studio tenemos como máximas las virtudes del deporte y del movimiento olímpico, del respeto a las

normas, del juego limpio y de la camaradería entre las personas que componen la empresa"

Sport Studio desarrolla sus actividades buscando conciliar sus legítimos intereses de rentabilidad, crecimiento y sostenibilidad con una política basada en el **compromiso:**

Compromiso con **nuestro personal**, de ofrecerles un empleo digno, estable y de calidad, que identifique su potencial y permita su promoción interna siempre en el ámbito de la corresponsabilidad.

Compromiso con **nuestros clientes** que confían en nuestra profesionalidad, rapidez y atención para ayudarles en la gestión de sus instalaciones deportivas.

Compromiso con **los usuarios** ofreciéndoles programas de actividad física desde todos los puntos de vista posibles del deporte, Sport Studio es salud, diversión, descanso, ocio, compañía, educación, bienestar, ...

Compromiso con **la sociedad** colaborando, con el deporte como herramienta, con cualquier entidad que promueva un mundo mejor y más justo.

Para desempeñar sus funciones y prestaciones, la organización, hace uso de sistemas de información que deben ser administrados con diligencia y protegidos de una forma efectiva y eficiente, frente a posibles daños accidentales o intencionados que pudieran afectar a las garantías de disponibilidad, autenticidad, integridad, confidencialidad y trazabilidad de las informaciones y los servicios prestados.

4 – ALCANCE

Esta Política será de aplicación y de obligado cumplimiento para todas las áreas de la organización, para sus recursos y para los procesos afectados por el Esquema Nacional de Seguridad y el Reglamento General de Protección de Datos, ya sean internos o externos vinculados a la entidad a través de contratos o acuerdos con terceros.

El alcance de esta política incluye:

Sistema de información que da soporte a los servicios de:

- Servicios prestados en materia de actividades deportivas
- Servicios prestados en materia de control de acceso
- Servicios prestados en materia del salvamento y socorrismo
- Servicios prestados en materia de gestión integral de instalaciones
- Servicios prestados en materia de limpieza y mantenimiento piscinas
- Asistencia técnico-deportiva para la celebración de eventos y pruebas deportivas
- Suministro de material deportivo,

Según su declaración de aplicabilidad vigente.

El alcance anterior incluye todos los servicios y sistemas tecnológicos, equipamiento, instalaciones y recursos utilizados en los procesos de producción de la organización.

5 – MARCO NORMATIVO

El marco normativo que afecta a la organización en el ámbito de la Política de Seguridad de la Información está integrado por las normas identificadas en el anexo:

"Legislación y Normativa aplicable"

6 – PRINCIPIOS BÁSICOS Y REQUISITOS MÍNIMOS [ENS]

6.1 – PRINCIPIOS BÁSICOS [ENS]

La presente Política de Seguridad de la Información se fundamenta en los siguientes principios básicos de protección que forman los pilares sobre los que han de asentarse todas las actuaciones en materia de seguridad de la información que realice la organización en su actividad.

La seguridad como proceso integral

La seguridad de la información es el resultado de un proceso integral que depende de todos y cada uno de los elementos humanos, técnicos, materiales, jurídicos y organizativos que intervienen en su tratamiento, evitando las actuaciones puntuales o tratamientos separados.
La política contará con el compromiso de todos los niveles directivos de modo que la seguridad de la información esté integrada y coordinada con las decisiones estratégicas de la organización.
Se contemplarán los aspectos de seguridad en todas las fases del ciclo de vida de los servicios, garantizando su seguridad por defecto. La seguridad se considerará como parte de la operativa habitual, estando presente y aplicando desde el diseño inicial de los sistemas de información.

Gestión de la seguridad basada en los riesgos

La gestión de la seguridad de la información está basada en la gestión de riesgos, cuyo objetivo debe ser mantener los niveles de riesgo dentro de unos niveles mínimos aceptables mediante el despliegue de las medidas de seguridad apropiadas y permanentemente actualizadas en todas las fases del ciclo de vida de las aplicaciones y servicios relacionados con el tratamiento de la información, estableciendo un equilibrio y proporcionalidad entre la naturaleza de los datos, los tratamientos realizados, los riesgos a los que estén expuestos y las medidas de seguridad aplicadas.

Prevención, detección, respuesta y conservación

La seguridad del sistema debe contemplar los aspectos de prevención, detección y respuesta para minimizar sus vulnerabilidades y conseguir que las amenazas sobre el mismo no se materialicen o que, en caso de hacerlo, no afecten gravemente a los datos que manejan los sistemas de información o los servicios que prestan.
Las medidas de prevención deberán eliminar o reducir la posibilidad de que las amenazas lleguen a materializarse, reduciendo la superficie de exposición, mientras que las medidas de detección deberán permitir descubrir posibles ciber-incidentes.

Las medidas de respuesta, gestionadas oportunamente, deberán permitir la restauración de la información y los servicios afectados por un incidente de seguridad.

El sistema de información garantizará la conservación de los datos e información en soporte electrónico y mantendrá disponibles los servicios durante todo el ciclo de vida de la información.

Existencia de líneas de defensa

Se establece una estrategia de protección constituida por múltiples capas de seguridad,

compuestas por medidas de naturaleza organizativa, operativa, física y lógica, dispuestas de tal forma que, si una de ellas falla, el sistema no se vea comprometido en su conjunto, minimizando el impacto final sobre el mismo.

Vigilancia continua y reevaluación periódica

La vigilancia continua permitirá la detección de actividades o comportamientos anómalos y su oportuna respuesta.
La evaluación permanente del estado de la seguridad de los activos permitirá medir su evolución, detectando vulnerabilidades e identificando deficiencias de configuración.

Las medidas de seguridad se reevaluarán y actualizarán periódicamente, adecuando su eficacia a la evolución de los riesgos y los sistemas de protección, pudiendo llegar a un replanteamiento de la seguridad, si fuese necesario.

Diferenciación de responsabilidades, coordinación y colaboración

La responsabilidad de la seguridad de los sistemas de información estará diferenciada de la responsabilidad sobre la explotación de los sistemas de información concernidos, siendo el Responsable de la Información quien determinará los requisitos de seguridad de la información tratada, el Responsable del Servicio quien determinará los requisitos de seguridad de los servicios prestados, el Responsable de Seguridad quien determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios, supervisará la implantación de las medidas necesarias para garantizar que se satisfacen los requisitos y reportará sobre estas cuestiones, y el Responsable del Sistema quien se encargará de desarrollar la forma concreta de implementar la seguridad en el sistema y de la supervisión de la operación diaria del mismo.

Todos los implicados en el proceso de seguridad actuarán de manera coordinada en la aplicación y control de las medidas de seguridad, bajo la coordinación del Responsable de la Seguridad. Esta coordinación se extenderá a todas las iniciativas y actuaciones de la organización, en esta materia.

6.2 – REQUISITOS MÍNIMOS [ENS]

Los principios básicos de protección se desarrollan aplicando los siguientes requisitos mínimos proporcionalmente a los riesgos identificados en cada sistema.

Organización e implantación del proceso de seguridad

La seguridad de los sistemas de información deberá comprometer a todos los miembros de la organización.

La política deberá ser conocida por todas las personas que formen parte de la organización e identificar a los responsables de velar por su cumplimiento: responsable de la información, responsable del servicio, responsable de la seguridad y responsable del sistema.

Análisis y gestión de los riesgos

La organización realizará la gestión de riesgos mediante la elaboración del análisis y tratamiento de riesgos a los que está expuesto el sistema, empleando una metodología reconocida.
Las medidas adoptadas para mitigar o suprimir los riesgos deberán estar justificadas y existirá una proporcionalidad entre ellas y los riesgos.

Gestión de personal

El personal, propio o ajeno, estará formado e informado de sus deberes, obligaciones y responsabilidades en materia de seguridad. Su actuación, que se supervisará para verificar que se siguen los procedimientos establecidos, aplicará las normas y procedimientos operativos de seguridad aprobados en el desempeño de sus cometidos.

El significado y alcance del uso seguro del sistema se concretará y plasmará en unas normas de seguridad que serán aprobadas por la dirección general a propuesta del Comité de Seguridad de la Información.

Profesionalidad

La seguridad de los sistemas de información estará atendida, revisada y auditada por personal cualificado, dedicado e instruido en todas las fases de su ciclo de vida: planificación, diseño, adquisición, construcción, despliegue, explotación, mantenimiento, gestión de incidencias y desmantelamiento.
La organización determinará los requisitos de formación y experiencia necesarios de este personal.

Autorización y control de los accesos

El acceso controlado a los sistemas de información deberá estar limitado a los usuarios, procesos, dispositivos u otros sistemas de información, debidamente autorizados, y exclusivamente a las funciones permitidas.

Protección de las instalaciones

Los sistemas de información y su infraestructura de comunicaciones deberán permanecer en áreas controladas y disponer de los mecanismos de acceso adecuados y proporcionales en función del análisis de riesgos.

Adquisición de productos de seguridad y contratación de servicios de seguridad

En la adquisición de productos de seguridad o contratación de servicios de seguridad de las tecnologías de la información y comunicaciones que vayan a ser empleados por la organización se utilizarán, de forma proporcionada a la categoría del sistema y al nivel de seguridad determinados, aquellos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición, observando los requisitos y criterios que establezca el Centro Criptológico Nacional.

Mínimo privilegio

Los sistemas de información serán diseñados otorgando los mínimos privilegios posibles para su correcto desempeño, proporcionando la funcionalidad imprescindible para que La organización alcance sus objetivos siendo las funciones de operación, administración y registro, las mínimas necesarias para ello y asegurando que sólo son desarrolladas por las personas autorizadas desde recursos asimismo autorizados.

Se aplicarán guías de configuración de seguridad para las diferentes tecnologías, adaptadas a la categorización del sistema, desactivando las funciones innecesarias o inadecuadas.

Integridad y actualización del sistema

Para la inclusión o modificación de cualquier elemento físico o lógico en el sistema, se requerirá autorización formal previa.

En todo momento se conocerá el estado de seguridad de los sistemas, en relación con las especificaciones de los fabricantes, las deficiencias de configuración, las vulnerabilidades y las actualizaciones que les afecten, así como la detección temprana de incidentes sobre aquellos, reaccionando con diligencia para gestionar el riesgo a la vista del estado de seguridad de los mismos.

Protección de la información almacenada y en tránsito

En la estructura y organización de la seguridad del sistema, se prestará especial atención a la información almacenada o en tránsito a través de entornos inseguros (equipos o dispositivos portátiles o móviles, periféricos, soportes, y redes abiertas, etc.). Se garantizará la conservación de los documentos electrónicos producidos por los sistemas. Toda la información en soporte no electrónico que sea causa o consecuencia directa de la información electrónica de los sistemas, también estará protegida al mismo nivel.

Prevención ante otros sistemas de información interconectados

Se protegerá el perímetro del sistema de información, especialmente, en el caso de conectarse a redes públicas, reforzándose las tareas de prevención, detección y respuesta

ante incidentes de seguridad. Se analizarán los riesgos derivados de la interconexión del sistema, a través de redes, con otros sistemas y se controlará su punto de unión.

Registro de actividad y detección de código dañino

Con el propósito de satisfacer el objeto del ENS, con plenas garantías del derecho al honor, a la intimidad personal y familiar y a la propia imagen de los afectados, y de acuerdo con la normativa sobre protección de datos personales, laboral, y demás disposiciones que resulten de aplicación, se registrarán las actividades de los usuarios, reteniendo la información estrictamente necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa.

Se podrá, en la medida estrictamente necesaria y proporcionada, analizar las comunicaciones entrantes o salientes, y únicamente para los fines de seguridad de la información, de forma que sea posible impedir el acceso no autorizado a las redes y sistemas de información, detener los ataques de denegación de servicio, evitar la distribución malintencionada de código dañino, así como otros daños a las antedichas redes y sistemas de información.

Cada usuario que acceda al sistema de información estará identificado de forma única, al objeto de conocer en todo momento, quién recibe derechos de acceso, de qué tipo son éstos, y quién ha realizado una determinada actividad.

Incidentes de seguridad

La organización dispondrá de procedimientos de gestión de incidentes de seguridad, incluyendo asimismo mecanismos de detección, criterios de clasificación, procedimientos de análisis y resolución, así como cauces de comunicación con las partes interesadas y el registro de las actuaciones. Este registro se utilizará para la mejora continua de la seguridad del sistema.

Continuidad de la actividad

Se dispondrá de copias de seguridad y se establecerán los mecanismos necesarios para garantizar la continuidad de las operaciones en caso de pérdida de los medios habituales.

Mejora continua del proceso de seguridad

Se actualizará y mejorará el proceso integral de seguridad de una forma continua, aplicando para ello criterios y métodos reconocidos en materia de seguridad de las TIC.

7 – ORGANIZACIÓN DE LA SEGURIDAD

La organización de la seguridad queda establecida mediante la identificación y definición de las diferentes responsabilidades en materia de gestión de la seguridad de los sistemas de información y la implantación de una estructura que las soporte.

Con carácter general, todos y cada uno de los usuarios de los sistemas de información de la organización son responsables de la seguridad de los activos de información mediante un uso correcto de los mismos, siempre de acuerdo con sus atribuciones profesionales.

Para una mejor respuesta a incidentes de seguridad, la organización mantendrá relaciones de cooperación en materia de seguridad con las autoridades competentes, proveedores de servicios informáticos o de comunicaciones, así como organismos públicos o privados dedicados a promover la seguridad de los sistemas de información.

En particular, la gestión de la seguridad de la información es responsabilidad específica de los siguientes responsables:

- Responsable de la Información y Responsables de los Servicios.
- Responsable de la Seguridad de la Información.
- Responsable del Sistema de Información.

- Comité de Seguridad de la Información.

Sus funciones se detallan en el anexo:

"**Organización de la seguridad de la información**"

La designación de las personas que desarrollan estas funciones se produce conforme a las instrucciones del Director Gerente de la organización.

Mecanismo de resolución de conflictos

Para la resolución de posibles conflictos de responsabilidad, o de otro tipo, que pudieran surgir, se tratarán y analizarán los asuntos pertinentes en el seno del Comité de Seguridad de la Información.

En caso de diferencias en la interpretación de esta Política o controversias no resueltas por el citado Comité, será el Director Gerente quien adoptará las decisiones necesarias, previo informe de dicho Comité.

8 – PROTECCIÓN DE DATOS PERSONALES

La organización, en el tratamiento de los datos personales, cumple con los principios y obligaciones de la normativa vigente, entre otra el Reglamento 679/2016, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la Protección de las Personas Físicas en lo que respecta al tratamiento de datos personales (Reglamento General de Protección de Datos-RGPD-) y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de derechos digitales, respetando, en todo caso, el derecho fundamental a la protección de datos personales, la intimidad y el resto de los derechos fundamentales reconocidos tanto en la legislación y tratados internacionales como en la Constitución vigente.

9 – DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

El cumplimiento de los objetivos marcados en esta Política de Seguridad se lleva a cabo mediante el desarrollo de documentación que componen las normas y procedimientos de seguridad asociados al Sistema de Gestión de la Seguridad de la Información.

Las normas serán aprobadas por el Comité de Seguridad de la Información.

El Responsable de Seguridad de la Información podrá aprobar procesos, procedimientos o instrucciones técnicas, dentro del ámbito de las TIC (tecnologías de la información y las comunicaciones).

La normativa de seguridad de la información estará disponible en la intranet a disposición de todos los miembros de la organización que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

10 – RELACIONES CON TERCERAS PARTES

Cuando la organización preste servicios a otros organismos o maneje información de los mismos, pondrá a su disposición esta política de seguridad de la información. Se establecerán canales de comunicación y coordinación entre los Responsables de Seguridad correspondientes, y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Asimismo, cuando la organización utilice servicios de terceros o ceda información a terceros, el responsable de esa relación les hará igualmente partícipes de esta política de seguridad y de la normativa e instrucciones de seguridad que ataña a dichos servicios o

información.

Dichos terceros quedarán sujetos a las obligaciones y medidas de seguridad establecidas en las respectivas normas e instrucciones, debiendo desarrollar sus propios procedimientos operativos para satisfacerla.
Se establecerán pautas específicas de prevención, detección, reporte y resolución de incidencias, siempre con el objetivo de que los terceros estén adecuadamente concienciados en materia de seguridad, al menos, al mismo nivel que el establecido en esta política de seguridad.

Cuando algún aspecto de esta política de seguridad no pueda ser satisfecho por los terceros, se requerirá un informe del Responsable de Seguridad de la Información que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por los responsables de la información y los servicios afectados, así como del responsable del tratamiento (previsto en el RGPD), antes de seguir adelante.

11 – INCUMPLIMIENTO DE LA POLÍTICA Y SANCIONES

Del incumplimiento de la Política de Seguridad de la Información y normas que la desarrollan podrán derivarse las consiguientes responsabilidades, que se determinarán con arreglo a la legislación aplicable tanto para los empleados como para los directivos de la organización.

12 – REVISIÓN DE LA POLÍTICA

Esta Política ha sido propuesta y revisada por el Comité de Seguridad de la Información.

Esta política será revisada por dicho Comité al menos una vez al año y siempre que haya cambios relevantes en la organización o en la legislación que corresponda, con el fin de asegurar que se mantiene el alineamiento necesario entre política, organización y legislación.