Los token de servicios y NFT (tokens no fungibles), en adelante criptoactivos, que se describen en este documento pueden ser de muy alto riesgo, incluso pueden perder totalmente su valor o liquidez o no ser canjeables por el servicio descrito, en caso de fracasar o interrumpirse el proyecto de StadioPlus. Los tokens y NFT (tokens no fungibles) que puedan adquirirse no serán custodiados por entidades legalmente autorizadas para prestar servicios de inversión y la tecnología de registro que está previsto utilizar (blockchain) es novedosa y puede conllevar importantes riesgos. El emisor de los criptoactivos es el único responsable del contenido del presente libro blanco de emisión de tokens. Este no ha sido revisado ni aprobado por ninguna autoridad competente de ningún Estado Miembro de la Unión Europea.

Riesgos

Un token lleva implícito diversos riesgos. A continuación mencionaremos algunos de ellos, pudiendo existir otros. Estos riesgos pueden generar la pérdida completa de los tokens, o de su valor. El poseedor del token y NFT (tokens no fungibles) asume y entiende perfectamente todos los riesgos que implica un token. En ningún caso, si el token pierde valor o cualquier otra cosa ocurre, el Emisor del token compensará al poseedor del token de alguna forma.

Producto de inversión de alto riesgo

1. El valor de las inversiones y el rendimiento obtenido de las mismas puede experimentar significativas variaciones al alza y a la baja, pudiendo perderse la totalidad del importe invertido.

2. Las inversiones en proyectos en etapas tempranas suponen un alto nivel de riesgo, por lo que resulta necesario entender adecuadamente su modelo de negocio.

3. Los criptoactivos del ámbito de la Circular 1/2022, de 10 de enero, de la Comisión Nacional del Mercado de Valores, relativa a la publicidad sobre criptoactivos presentados como objeto de inversión no están cubiertos por mecanismos de protección al cliente como el Fondo de Garantía de Depósitos o el Fondo de Garantía de Inversores.

4. Los precios de los criptoactivos se constituyen en ausencia de mecanismos que aseguren su correcta formación, como los presentes en los mercados regulados de valores.

5. Muchos criptoactivos pueden verse carentes de la liquidez necesaria para poder deshacer una inversión sin sufrir pérdidas significativas, dado que su circulación entre inversores, tanto minoristas como profesionales, puede ser muy limitada.

Riesgos propios de la tecnología

6. Las tecnologías de registros distribuidos se encuentran todavía en un estadio temprano de maduración, habiendo sido muchas de estas redes creadas recientemente,por lo que pueden no estar suficientemente probadas y existir fallos significativos en su funcionamiento y seguridad.

Riesgo de servicios de wallet incompatibles: El proveedor de servicios de cartera digital o cartera digital utilizados para recibir tokens debe cumplir con el estándar de token ERC-20 para ser técnicamente compatible con dichos tokens. El hecho de no garantizar dicha conformidad puede tener como resultado que el suscriptor pierda acceso a sus tokens.

7. El registro de las transacciones en las redes basadas en tecnologías de registros distribuidos funciona a través de protocolos de consenso que pueden ser susceptibles a ataques que intenten modificar dicho registro y, en caso de tener éxito estos ataques, no existiría un registro alternativo que respalde dichas transacciones ni por tanto a los saldos correspondientes a las claves públicas, pudiéndose perder la totalidad de los criptoactivos.

8. Las facilidades de anonimato que pueden aportar los criptoactivos los convierten en un objetivo para los ciberdelincuentes, ya que en el caso de robar credenciales o claves privadas pueden transferir los criptoactivos a direcciones que dificulten o impidan su recuperación.

9. La custodia de los criptoactivos supone una responsabilidad muy relevante ya que pueden perderse en su totalidad en el caso de robo o pérdida de las claves privadas.

No obstante, la compañía no realiza custodia de criptoactivos en nombre de sus clientes y serán éstos quienes realicen la custodia de los criptoactivos por su cuenta y riesgos, bien mediante un wallet de su titularidad o mediante un servicio de terceros, que en ningún caso tendrá relación con la compañía.

Riesgos legales

La aceptación de los criptoactivos como medio de cambio es aún muy limitada y no existe obligación legal de aceptarlos.

1. Riesgos asociados a la oferta y negociación

Riesgo de liquidez: Cabe la posibilidad de que no se consiga incluir el token y NFT (tokens no fungibles) en cuestión a algún mercado secundario o que exista falta de liquidez en mercados OTC (over the counter). La compañía no se hace responsable de las fluctuaciones que el token en cuestión pueda sufrir en cualquier tipo de mercado o de que tales tipos de mercado permitan poner a cotizar el token, pudiendo ello conllevar riesgos de iliquidez. Incluso en el caso de que el token llegase a cotizar en la plataforma de un tercero, dichas plataformas pueden no disponer de suficiente liquidez o incluso encontrarse ante riesgos de cambios regulatorios o de cumplimiento normativo, siendo por tanto susceptibles de falla, caída o manipulación. Además, en la medida en que la plataforma de un tercero ponga a cotizar el token en cuestión, otorgando un valor de cambio al token o NFT (tokens no fungibles)(ya sea en criptoactivos o dinero fiduciario), dicho valor puede padecer volatilidades. Como comprador en este tipo de activos, asume todos los riesgos asociados a la especulación y riesgos anteriormente mencionados. Este tipo de activos no

están cubiertos por mecanismos de protección al cliente como el Fondo de Garantía de Depósitos o el Fondo de Garantía de Inversores. Además, los precios no se constituyen por medio de mecanismos que aseguren su correcta formación a diferencia de los que encontramos en los mercados regulados. La aceptación de los criptoactivos como medio de cambio es aún muy limitada y no existe obligación legal de aceptarlos

2. Riesgos Asociados a la ejecución del proyecto y/o al Emisor

Riesgo de información a futuro: Cierta información contenida en el Whitepaper de la compañía es de carácter prospectivo, incluyendo las proyecciones financieras y las proyecciones de crecimiento del negocio. Dicha información a futuro se basa en lo que la gerencia del Emisor cree que son suposiciones razonables, y no puede haber seguridad de que los resultados sean reales. Los eventos futuros podrían diferir sustancialmente de los anticipados.

Riesgo regulatorio: La tecnología blockchain permite nuevas formas de interacción y es posible que ciertas jurisdicciones apliquen las regulaciones existentes o introduzcan nuevas regulaciones que aborden las aplicaciones basadas en la tecnología blockchain, que pueden ser contrarias a la configuración actual de los smart contracts y que pueden, entre otras cosas, dar lugar a modificaciones sustanciales en los mismos, incluyendo su terminación y la pérdida de tokens para el suscriptor.

Riesgo de fracaso o abandono del proyecto: El desarrollo del proyecto planteado por el Emisor en el presente documento puede verse impedido y cesado por diferentes razones, incluyendo la falta de interés por parte del mercado, falta de financiación, falta de éxito comercial o perspectivas (por ejemplo, provocadas por proyectos

competidores). La presente emisión de tokens no garantiza que los objetivos marcados en el presente documento lleguen a ser desarrollados total o parcialmente.

Riesgo de compañías competidoras: Es posible que otras empresas pudieran prestar servicios similares al de la compañía. La compañía podría competir con dichas otras empresas, pudiendo ello impactar negativamente en los servicios prestados por ésta.

3. Riesgos asociados a los tokens y NFT (tokens no fungibles) y la tecnología utilizada

Riesgo de software: El código informático (smart contract) por el que se comercializan los referidos tokens están basados en el protocolo Ethereum o/y Binance Smart Chain en el que se decida emitir el token como lo establece el whitepaper. Cualquier mal funcionamiento, caída o abandono del proyecto Ethereum o red elegida donde se desarrolle el token puede provocar efectos adversos en el funcionamiento de los tokens en cuestión. Por otro lado, los avances tecnológicos en general y en criptografía en particular, tales como el desarrollo de la computación cuántica pueden traer consigo riesgos que deriven en el mal funcionamiento de estos tokens. Los smart contracts y el software en el que se basan se encuentran en una etapa temprana de desarrollo. No existe garantía ni forma de asegurar que la emisión de tokens y su posterior comercialización pueda ser interrumpida o que padezcan cualquier otro tipo de error, por lo que hay un riesgo inherente de que se produzcan defectos, fallas y vulnerabilidades que puedan dar lugar a la pérdida de los fondos aportados o de los tokens obtenidos. Existe un riesgo de ataques de piratas o hackers informáticos en la infraestructura tecnológica utilizada por el Emisor y en las redes y

tecnologías esenciales. Como resultado, el Emisor puede ser impedido parcial, temporal o incluso permanentemente de llevar a cabo sus actividades comerciales.

En el caso de los mecanismos de consenso de prueba de trabajo en Ethereum, podría darse el caso de que alguien pudiese controlar más del 50% del poder computacional de los mineros de la cadena de bloques en un llamado ataque del 51% y, por lo tanto, toma el control de la red (la cadena de bloques). Utilizando más del 50% del poder minero (poder hash), el atacante siempre representará a la mayoría, lo que significa que puede imponer su versión de la cadena de bloques. En principio, esto también es posible con menos del 51% de la potencia de minería.

Una vez que el atacante haya ganado el control de la red, podría revertir o redirigir las transacciones que inició, de modo que sería posible "duplicar el gasto" (es decir, realizar transacciones múltiples del mismo token). El atacante también puede bloquear las transacciones de otros negándose la confirmación. Podrían, además, darse otros ataques informáticos en la blockchain de Ethereum, el software y/o el hardware utilizado por el Emisor.

Además de los ataques de hackers informáticos, existe el riesgo de que los empleados del Emisor o terceros puedan sabotear los sistemas tecnológicos, lo que puede provocar el fallo de los sistemas de hardware y/o software del Emisor. Esto también podría acarrear un impacto negativo en las actividades comerciales del Emisor.