Proyecto de Reglamento

Fiabilidad y seguridad de la información de los sistemas de juegos de azar en virtud de la Ley sobre los juegos de azar

Índice

1 Marco jurídico, ámbito de aplicación y definiciones

1.1 La facultad de la autoridad supervisora para dictar órdenes

El derecho de la autoridad de supervisión a emitir una orden vinculante se basa en el artículo 44, apartado 6, de la Ley (xx/2025) sobre los juegos de azar. De acuerdo con dicho apartado, la autoridad de supervisión podrá emitir reglamentaciones más detalladas sobre la fiabilidad de los sistemas de juegos de azar, los equipos de lotería y los métodos de lotería utilizados en la explotación de los juegos de azar, sobre los requisitos técnicos para garantizar el carácter aleatorio del sorteo, sobre la forma y el contenido más detallados de la investigación y la aprobación del organismo de inspección, y sobre las condiciones que el organismo de inspección debe cumplir para ser aprobado por la Autoridad.

Según el artículo 57 de la Ley sobre los juegos de azar, la autoridad de supervisión es la Autoridad de Autorización y Supervisión. Según el artículo 106 de la Ley, la Dirección Nacional de la Policía actuará como autoridad competente a la que se refiere el artículo 57 hasta el 31 de diciembre de 2026.

1.2 Legislación

Las siguientes reglamentaciones son relevantes para el objeto del presente Reglamento:

- Ley (xx/2025) sobre los juegos de azar
- Ley (434/2003) sobre el procedimiento administrativo
- Ley (1050/2018) sobre la protección de datos
- Reglamento general de protección de datos de la UE (2016/679)

1.3 Ámbito de aplicación

Esta disposición se aplica a una persona física o jurídica a que se refiere el capítulo 1, artículo 2, apartado 1, de la Ley sobre los juegos de azar a la que se haya concedido una licencia exclusiva o una licencia para actividades de juegos de azar en virtud de la Ley sobre los juegos de azar.

La licencia exclusiva se rige por el artículo 5 de la Ley sobre los juegos de azar y la licencia de juegos de azar se rige por el artículo 6.

1.4 Definiciones

A los efectos de esta disposición, se aplicarán las siguientes definiciones. A efectos del presente Reglamento:

- *licencia exclusiva*: una licencia concedida para las formas de juegos de azar según el artículo 5 de la Ley sobre los juegos de azar;
- *licencia de juegos de azar*: una licencia concedida para los tipos de juegos de azar según el artículo 6 de la Ley sobre los juegos de azar;
- *transacción de juegos de azar*: la apuesta apostada por el jugador en el juego, la opción de resultado elegida por el jugador, las elecciones realizadas por el jugador que son pertinentes para el resultado del juego y los resultados de los mercados y sorteos, así como cualquier ganancia y pérdida registrada en el sistema de juegos de azar del titular de una licencia exclusiva o de una licencia de juegos de azar;
- *transacciones de la cuenta del jugador*: entradas en la cuenta.
- *sistema de juegos de azar*: un sistema de información en línea utilizado por el operador de juegos de azar o en su nombre para la explotación de juegos de azar;

2 Acreditación de un organismo de inspección

El titular de la licencia es responsable de la fiabilidad de sus dispositivos de lotería y sistemas de juego, así como de llevar a cabo las auditorías necesarias para garantizar dicha fiabilidad. La evaluación de la fiabilidad y la seguridad la lleva a cabo un organismo de inspección externo acreditado. El organismo de inspección estará acreditado de conformidad con el Reglamento (CE) n.º 765/2008 del Parlamento Europeo y del Consejo por el que se establecen los requisitos de acreditación y vigilancia del mercado relativos a la comercialización de los productos y por el que se deroga el Reglamento (CEE) n.º 339/93.

La acreditación puede ser concedida a los organismos de inspección por el organismo nacional de acreditación FINAS (Servicio Finlandés de Acreditación). Un organismo de acreditación extranjero también puede actuar como organismo de acreditación si es miembro del Acuerdo de Reconocimiento Multilateral de la Organización Europea de Acreditación (EA MLA) en el ámbito de competencia pertinente. El titular de la licencia está obligado a garantizar que el operador externo que lleve a cabo la auditoría tenga una acreditación válida.

3 Prácticas generales de seguridad de la información

El titular de la licencia es responsable de la seguridad de la información, la protección de datos y otras características técnicas de fiabilidad de sus propios sistemas de juegos de azar. El titular de la licencia deberá seguir buenas prácticas de seguridad de la información en sus operaciones y esforzarse por minimizar las amenazas para la seguridad de la información, las violaciones de la seguridad de los datos y otros problemas que puedan poner en peligro la fiabilidad de los sistemas de juegos de azar. El titular de la licencia también está obligado a supervisar los factores mencionados

anteriormente fuera de las inspecciones periódicas a las que se refiere el presente Reglamento, con el fin de garantizar la fiabilidad de sus sistemas.

4 Organismo de inspección que lleva a cabo las pruebas de seguridad de la información

El titular de la licencia está obligado a realizar pruebas de seguridad en sus sistemas de juego cada dos años. Los resultados de las pruebas de seguridad de la información deberán remitirse a la autoridad de control. Las pruebas de seguridad de la información y sus resultados no podrán tener más de dos años de antigüedad.

Las pruebas de seguridad de la información serán realizadas por un organismo de inspección externo acreditado de conformidad con las normas ISO/IEC 17025, ISO/IEC 17065 o ISO/IEC 17020, tal como se especifica en la sección 2 del presente Reglamento. Las pruebas de seguridad de la información prestarán especial atención a la protección y la integridad de los componentes del sistema de juego aleatorio, a la protección de los componentes que contienen datos personales y a la protección de los componentes relacionados con los pagos.

El organismo de inspección responsable de realizar las pruebas de seguridad de la información y su personal deberán ser competentes y adecuados para llevar a cabo las pruebas. La competencia necesaria para llevar a cabo las pruebas de seguridad de la información puede demostrarse, entre otras cosas, mediante experiencia profesional previa en pruebas de seguridad de la información, formación o certificados del sector generalmente reconocidos. El titular de la licencia está obligado a garantizar que las personas que realizan las pruebas estén cualificadas para realizar pruebas de seguridad de la información y, previa solicitud, a demostrar sus cualificaciones.

Se designará a una persona encargada de la realización de las pruebas de seguridad, que será responsable de su correcta ejecución. El informe final de la prueba de seguridad de la información deberá ser firmado y validado por la persona designada y presentado a la autoridad supervisora.

En el contexto de las pruebas de seguridad de la información, se someterán a prueba, como mínimo, los siguientes componentes, así como las vulnerabilidades o incidentes relacionados:

- Posibilidad de manipulación de los componentes aleatorios.
- Acceso a la base de datos de clientes
- Capacidad de influir en el resultado de los juegos
- Capacidad para influir en los sistemas de pago o en las transacciones de pago.
- Acceso no autorizado a servidores utilizados para almacenar transacciones de apuestas y transacciones de cuentas de jugadores.

- Capacidad de editar los datos del evento de juego archivado o del evento de cuenta de juego
- Modificación o destrucción de los registros relativos a los sistemas de juego

4.1 Ámbito competencial

El organismo de inspección acreditado que realice la auditoría deberá contar con el área de competencia para juegos de azar en su acreditación ISO/IEC. El ámbito de competencia debe cubrir los requisitos establecidos por la legislación finlandesa sobre juegos de azar y los reglamentos técnicos de la autoridad de supervisión.

Hasta el 1 de enero de 2027, la autoridad de supervisión podrá aceptar una acreditación que incluya un ámbito de competencia evaluado y concedido sobre la base de reglamentaciones técnicas emitidas para los sistemas de juegos de azar de Dinamarca o Suecia.

5 Renovación de las pruebas de seguridad de la información

El titular de la licencia deberá presentar los resultados de las pruebas de seguridad de la información aprobadas a la autoridad supervisora. El titular de la licencia no podrá iniciar la explotación de juegos de azar antes de que haya superado con éxito las pruebas de seguridad. El resultado de la prueba de seguridad de la información no deberá tener más de dos años de antigüedad.

La autoridad de supervisión podrá, a su discreción, conceder tiempo adicional para la aplicación de pruebas de seguridad, durante el cual podrá continuar la explotación de juegos de azar.

6 Prueba de seguridad de la información rechazada

El organismo de inspección que realice la prueba de seguridad de la información deberá evaluar las vulnerabilidades identificadas durante la prueba de seguridad de la información y su importancia para la fiabilidad del sistema de juego. Las vulnerabilidades identificadas durante la evaluación deben evaluarse utilizando la calculadora CVSS v3 (Common Vulnerability Scoring System Calculator, versión 3) proporcionada por el Instituto Nacional de Tecnología (NIST). Para la calculadora CVSS v3, la gravedad de la vulnerabilidad se evaluará utilizando métricas de puntuación base. Si durante las pruebas de seguridad se detectan vulnerabilidades con un valor CVSS calculado superior a 5,0, la prueba no se puede considerar satisfactoria.

Si no se aprueba la prueba de seguridad de la información del titular de la licencia, este deberá adoptar inmediatamente medidas para subsanar las vulnerabilidades de seguridad de la información identificadas. El titular de la licencia deberá notificar la prueba de seguridad de la información rechazada a la autoridad de supervisión.

El titular de la licencia deberá llevar a cabo una nueva prueba de seguridad en un plazo de noventa días a partir de la prueba de seguridad de la información rechazada. No es necesario llevar a cabo nuevas pruebas de seguridad de la información en todo el sistema de juegos de azar; en su lugar, las pruebas de seguridad de la información pueden centrarse en las deficiencias que provocaron el rechazo. En relación con la renovación de las pruebas de seguridad de la información, el organismo de inspección debe asegurarse de que se han corregido las vulnerabilidades previamente identificadas como motivos de rechazo.

La implementación de juegos de azar no podrá comenzar antes de que se hayan llevado a cabo pruebas de seguridad aprobadas y válidas.

7 Análisis de vulnerabilidades

Además de las pruebas de seguridad, los titulares de licencias están obligados a supervisar la seguridad de sus propios sistemas mediante análisis regulares de vulnerabilidad. El objetivo de los análisis de vulnerabilidades es garantizar que los sistemas de juego utilizados por el titular de la licencia no tengan ninguna vulnerabilidad de seguridad externa que pueda ser aprovechada para llevar a cabo ataques contra los sistemas de juego.

El titular de la licencia está obligado a realizar un análisis externo de vulnerabilidades una vez al año y a comunicar los resultados a la autoridad supervisora. El análisis de vulnerabilidades podrá ser realizado por un organismo de inspección externo acreditado de conformidad con las normas ISO/IEC 17025, ISO/IEC 17065 o ISO/IEC 17020, tal como se especifica en el apartado 2 del presente Reglamento.

El titular de la licencia está obligado a corregir las vulnerabilidades detectadas durante el análisis de vulnerabilidades con actualizaciones u otras medidas de mitigación urgentes si no se dispone de actualizaciones correctivas. El método de evaluación descrito en la sección 6 se aplicará a las vulnerabilidades de seguridad detectadas durante los análisis de vulnerabilidades. Si el valor CVSS calculado de la vulnerabilidad externa identificada es superior a 5,0, el titular de la licencia adoptará medidas inmediatas para subsanar las vulnerabilidades.

El organismo de inspección responsable de realizar el análisis de vulnerabilidades y su personal deben ser competentes y adecuados para llevar a cabo las pruebas. La competencia necesaria para llevar a cabo análisis de vulnerabilidades puede demostrarse mediante experiencia profesional previa en pruebas de seguridad de la información, experiencia en el uso de escáneres de vulnerabilidades, formación o certificados del sector generalmente reconocidos, entre otros. El titular de la licencia está obligado a garantizar que las personas que realizan las pruebas estén cualificadas para llevar a cabo análisis de vulnerabilidades y, previa solicitud, a demostrar sus cualificaciones.

Se debe designar a una persona responsable de realizar el análisis de vulnerabilidades para garantizar que se lleve a cabo de manera adecuada. El informe final del análisis de vulnerabilidades deberá ser firmado y validado por la persona responsable y presentado a la autoridad supervisora.

8 Análisis de vulnerabilidades realizados en relación con las pruebas de seguridad de la información

El titular de la licencia puede realizar análisis de vulnerabilidades como parte de las pruebas de seguridad de la información. Los mismos requisitos se aplican a los análisis de vulnerabilidades realizados como parte de las pruebas de seguridad de la información que a otros análisis de vulnerabilidades.

9 Corrección de vulnerabilidades

El titular de la licencia está obligado a supervisar periódicamente la seguridad de la información de sus propios sistemas de juegos de azar, incluso fuera de las pruebas de seguridad de la información, y a corregir las vulnerabilidades que comprometen la fiabilidad cuando se disponga de correcciones u otros métodos de mitigación.

Si no es posible subsanar rápidamente las vulnerabilidades, el titular de la licencia tratará de utilizar los medios disponibles para combatir las vulnerabilidades y minimizar el impacto.

Si el valor de la puntuación base CVSS v3 de la vulnerabilidad externa detectada es inferior a 5,0, el titular de la licencia podrá aplicar correcciones y evaluar la urgencia de las mismas a su propia discreción.

10 Uso de los certificados expedidos

Un organismo de inspección acreditado aprobado por la autoridad de supervisión responsable de llevar a cabo las pruebas de seguridad de la información o el análisis de vulnerabilidades podrá utilizar certificados u otros certificados concedidos al titular de la licencia de software de juegos de azar como parte de su inspección. Si el organismo de inspección utiliza certificados existentes como parte de la inspección, deberá evaluar si los certificados pueden considerarse pruebas suficientemente fiables de la fiabilidad y la seguridad de la información del sistema de juego del titular de la licencia de software de juego.

11 Discrepancias

El titular de la licencia está obligado a notificar sin demora a la autoridad de supervisión cualquier violación de la seguridad de la información o de la protección de datos que detecte si existen motivos para sospechar que la fiabilidad de los sistemas de juegos de azar o de los equipos de lotería utilizados por el titular de la licencia se ha visto comprometida.

Los titulares de licencias no estarán obligados a notificar incidentes menores de seguridad o protección de datos a la autoridad de supervisión de los juegos de azar cuando la eficacia estimada del incidente sea de naturaleza limitada o cuando no se considere que el incidente tenga un impacto significativo en la fiabilidad de los sistemas de juegos de azar.

12 Entrada en vigor

El presente Reglamento entrará en vigor el X [mes] 2026.

Dirección Nacional de la Policía
Administración de Juegos de Azar
Konepajankatu 2, PL 50, 11101 Riihimäki
Teléfono +358 295 480 181, poliisi.fi