Projeto de regulamento

Fiabilidade e segurança da informação dos sistemas de jogo ao abrigo da Lei relativa ao jogo

Índice

1 Quadro jurídico, âmbito de aplicação e definições

1.1 Competência da autoridade de supervisão para emitir regulamentos

O direito de a autoridade de supervisão para emitir um regulamento vinculativo baseia-se no artigo 44.º, n.º 6, da Lei relativa ao jogo (xx/2025). Em conformidade com o referido número, a autoridade de supervisão pode emitir regulamentos mais circunstanciados relativos à fiabilidade dos sistemas de jogo, dos dispositivos de lotaria e dos métodos de lotaria utilizados na execução de jogos, bem como relativos aos requisitos técnicos para garantir a aleatoriedade do sorteio, relativos à forma e ao conteúdo mais pormenorizados da investigação e aprovação do organismo de controlo e relativos às condições que o organismo de controlo deve satisfazer para que a autoridade o aprove.

Em conformidade com o artigo 57.º da Lei relativa ao jogo, a autoridade de supervisão é a Agência de Supervisão finlandesa. Nos termos do artigo 106.º da lei, o Serviço Nacional de Polícia atua como a autoridade competente a que se refere o artigo 57.º até 31 de dezembro de 2026.

1.2 Legislação

Os seguintes atos são pertinentes para o objeto do presente regulamento:

- Lei relativa ao jogo (xx/2025)
- Lei do Procedimento Administrativo (434/2003)
- Lei de Proteção de Dados (1050/2018)
- Regulamento Geral sobre a Proteção de Dados da UE (2016/679)

1.3 Âmbito de aplicação

O presente regulamento é aplicável a uma pessoa singular ou coletiva a que se refere o capítulo 1, ponto 2, subponto 1, da Lei relativa ao jogo, à qual tenha sido concedida uma licença exclusiva ou uma licença para atividades de jogo nos termos da Lei relativa ao jogo.

A licença exclusiva é regida pelo artigo 5.º da Lei relativa ao jogo e a licença de jogo é regida pelo artigo 6.º.

1.4 Definições

Para efeitos do presente regulamento, são aplicáveis as seguintes definições. Para efeitos do presente regulamento, entende-se por:

- *«Licença exclusiva»*, uma licença concedida para os tipos de jogo na aceção do artigo 5.º da Lei relativa ao jogo;

- *«Licença de jogo»*, uma licença concedida para os tipos de jogo na aceção do artigo 6.º da Lei relativa ao jogo;
- *«Transação de jogo»*, a aposta efetuada pelo jogador no jogo, a opção de resultado escolhida pelo jogador, as escolhas feitas pelo jogador que sejam relevantes para o resultado do jogo e os resultados das apostas e sorteios, bem como quaisquer ganhos e perdas registados no sistema de jogo do titular de uma licença exclusiva ou licença de jogo;
- *«Transação da conta do jogador»*, as entradas na conta.
- *«Sistema de jogo»*, um sistema de informação em linha utilizado pelo operador de jogos, ou em seu nome, para a exploração de jogos.

2 Acreditação de um organismo de controlo

O titular da licença é responsável pela fiabilidade dos seus dispositivos de lotaria e sistemas de jogo, bem como pela realização de auditorias para garantir essa fiabilidade. A avaliação da fiabilidade e segurança é efetuada por um organismo de controlo externo acreditado. O organismo de controlo deve ser acreditado em conformidade com o Regulamento (CE) n.º 765/2008 do Parlamento Europeu e do Conselho que estabelece os requisitos de acreditação e fiscalização do mercado relativos à comercialização de produtos, e que revoga o Regulamento (CEE) n.º 339/93.

A acreditação pode ser concedida aos organismos de controlo pelo organismo nacional de acreditação, o Serviço de Acreditação finlandês (FINAS). Um organismo estrangeiro de acreditação também pode atuar como organismo de acreditação se for membro do acordo de reconhecimento multilateral da Organização Europeia de Acreditação (ARM OEA) no domínio de competência relevante. O titular da licença é obrigado a assegurar que o operador externo que efetua a auditoria possui uma acreditação válida.

3 Práticas gerais de segurança da informação

O titular da licença é responsável pela segurança da informação, pela proteção de dados e por outras características técnicas de fiabilidade dos seus próprios sistemas de jogo. O titular da licença deve respeitar as boas práticas de segurança da informação nas suas operações e esforçar-se por minimizar as ameaças à segurança da informação, as violações de dados e outros problemas que possam comprometer a fiabilidade dos sistemas de jogo. O titular da licença também é obrigado a monitorizar os aspetos referidos anteriormente fora das auditorias regulares referidas no presente regulamento, a fim de assegurar a fiabilidade dos seus sistemas.

4 Organismo de controlo que efetua testes de segurança da informação

O titular da licença é obrigado a efetuar testes de segurança nos seus sistemas de jogo de dois em dois anos. O resultado dos testes de segurança da informação deve ser apresentado à autoridade de supervisão. Os testes de segurança da informação e os seus resultados não podem ter mais de dois anos.

Os testes de segurança da informação devem ser efetuados por um organismo de controlo externo acreditado, em conformidade com as normas ISO/IEC 17025, ISO/IEC 17065 ou ISO/IEC 17020, conforme estabelecido no n.º 2 do presente regulamento. Os testes de segurança da informação devem centrar-se na proteção e integridade dos componentes de geração de resultados aleatórios do sistema de jogo, na proteção dos componentes que contêm dados pessoais e na proteção dos componentes relacionados com os pagamentos.

O organismo de controlo responsável pela realização dos testes de segurança da informação e o seu pessoal devem ser qualificados e adequados para efetuar os testes. A competência necessária para efetuar testes de segurança da informação pode ser demonstrada, entre outros aspetos, pela experiência profissional anterior em testes de segurança da informação, formação ou certificados do setor geralmente reconhecidos. O titular da licença é obrigado a assegurar que as pessoas que efetuam os testes são qualificadas para efetuar os testes de segurança da informação e, mediante pedido, a comprovar as suas qualificações.

Deve ser designada uma pessoa responsável pela realização dos testes de segurança, à qual cabe a sua correta realização. A pessoa responsável deve assinar e validar o relatório final dos testes de segurança da informação e apresentá-lo à autoridade de supervisão.

No contexto dos testes de segurança da informação, devem ser testados, no mínimo, os seguintes componentes, bem como as vulnerabilidades ou os incidentes conexos:

- Possibilidade de manipulação dos componentes aleatórios
- Acesso à base de dados de clientes
- Capacidade de influenciar o resultado dos jogos
- Capacidade de influenciar os sistemas de pagamento ou as operações de pagamento
- Acesso não autorizado aos servidores utilizados para armazenar as transações de jogos e as transações de contas de jogadores
- Capacidade de alterar dados arquivados relativos a eventos de jogos ou a contas de jogos
- Alteração ou destruição de registos relacionados com os sistemas de jogo

4.1 Domínio de competência

O organismo de controlo acreditado que efetua a auditoria deve ter competência no domínio dos jogos de fortuna e azar na sua acreditação ISO/IEC. O domínio de competência deve abranger os requisitos estabelecidos pela legislação finlandesa em matéria de jogos de fortuna e azar e os regulamentos técnicos da autoridade de supervisão.

Até 1 de janeiro de 2027, a autoridade de supervisão pode aceitar uma acreditação que inclua um âmbito de competência avaliado e concedido com base nos regulamentos técnicos emitidos para os sistemas de jogo dinamarqueses ou suecos.

5 Renovação dos testes de segurança da informação

O titular da licença deve apresentar os resultados dos testes de segurança da informação aprovados à autoridade de supervisão. O titular da licença não pode dar início à exploração de jogos antes de ser aprovado nos testes de segurança. O resultado dos testes de segurança da informação não deve ter mais de dois anos.

A autoridade de supervisão pode, a seu critério, conceder tempo adicional para a realização dos testes de segurança, durante o qual a exploração de jogos pode continuar.

6 Teste de segurança da informação reprovado

O organismo de controlo que efetua os testes de segurança da informação deve avaliar as vulnerabilidades identificadas durante os testes de segurança da informação e a sua importância para a fiabilidade do sistema de jogo. As vulnerabilidades identificadas durante a avaliação devem ser avaliadas utilizando a calculadora do CVSS v3 (versão 3 do sistema de pontuação de vulnerabilidade comum) fornecida pelo Instituto Nacional de Tecnologia (NIST). No que diz respeito à calculadora do CVSS v3, a gravidade da vulnerabilidade deve ser avaliada utilizando métricas de pontuação de base. Caso sejam detetadas vulnerabilidades com um valor CVSS calculado superior a 5,0 durante o teste de segurança, o teste não pode ser considerado aprovado.

Se o teste de segurança da informação não for aprovado, o titular da licença deve tomar imediatamente medidas para corrigir as vulnerabilidades de segurança da informação identificadas. O titular da licença deve comunicar o teste de segurança da informação reprovado à autoridade de supervisão.

O titular da licença deve efetuar um novo teste de segurança no prazo de 90 dias após o teste de segurança da informação reprovado. Não é necessário efetuar novos testes de segurança da informação em todo o sistema de jogo; ao invés, o teste de segurança da informação pode ser orientado para as deficiências que resultaram na reprovação. No âmbito da realização do novo teste de segurança da informação, o organismo de controlo deve assegurar que as vulnerabilidades anteriormente identificadas como motivos para a reprovação foram corrigidas.

A exploração de jogos não pode começar antes da realização de testes de segurança aprovados e válidos.

7 Análises das vulnerabilidades

Para além dos testes de segurança, os titulares de licenças são obrigados a monitorizar a segurança dos seus próprios sistemas através de análises regulares das vulnerabilidades. O objetivo das análises das vulnerabilidades é garantir que os sistemas de jogo utilizados pelo titular da licença não apresentem quaisquer vulnerabilidades de segurança externas que possam ser exploradas para realizar ataques contra os sistemas de jogo.

O titular da licença é obrigado a efetuar uma análise das vulnerabilidades externas uma vez por ano e a comunicar os resultados à autoridade de supervisão. A análise das vulnerabilidades pode ser efetuada por um organismo de controlo externo acreditado, em conformidade com as normas ISO/IEC 17025, ISO/IEC 17065 ou ISO/IEC 17020, conforme estabelecido no n.º 2 do presente regulamento.

O titular da licença é obrigado a corrigir as vulnerabilidades detetadas durante a análise das vulnerabilidades com atualizações ou outras medidas de mitigação urgentes, caso não estejam disponíveis atualizações corretivas. O método de avaliação descrito no n.º 6 deve ser aplicado às vulnerabilidades de segurança detetadas durante as análises das vulnerabilidades. Caso o valor CVSS calculado da vulnerabilidade externa identificada for superior a 5,0, o titular da licença deve tomar medidas imediatas para corrigir as vulnerabilidades.

O organismo de controlo responsável pela realização da análise das vulnerabilidades e o seu pessoal devem ser qualificados e adequados para efetuar as análises. A competência necessária para efetuar análises das vulnerabilidades pode ser demonstrada, entre outros aspetos, pela experiência profissional anterior em testes de segurança da informação, experiência na realização de análises das vulnerabilidades, formação ou certificados do setor geralmente reconhecidos. O titular da licença é obrigado a assegurar que as pessoas que efetuam os testes são qualificadas para efetuar análises das vulnerabilidades e, mediante pedido, a comprovar as suas qualificações.

Deve ser designada uma pessoa responsável pela realização da análise das vulnerabilidades para assegurar que esta seja efetuada corretamente. A pessoa responsável deve assinar e validar o relatório final da análise das vulnerabilidades e apresentá-lo à autoridade de supervisão.

8 Análises das vulnerabilidades efetuadas no âmbito dos testes de segurança da informação

O titular da licença pode efetuar análises das vulnerabilidades como parte dos testes de segurança da informação. Os mesmos requisitos aplicam-se às análises das vulnerabilidades efetuadas como parte dos testes de segurança da informação e a outras análises das vulnerabilidades.

9 Correção de vulnerabilidades

O titular da licença é obrigado a monitorizar regularmente a segurança da informação dos seus próprios sistemas de jogo, incluindo fora dos testes de segurança da informação, e a corrigir as vulnerabilidades que comprometam a fiabilidade, sempre que estiverem disponíveis correções ou outros métodos de mitigação.

Caso não seja possível corrigir rapidamente as vulnerabilidades, o titular da licença deve procurar utilizar os meios disponíveis para eliminar as vulnerabilidades e atenuar o seu impacto.

Se o valor da pontuação de base CVSS v3 da vulnerabilidade externa detetada for inferior a 5,0, o titular da licença pode, a seu critério, aplicar correções e avaliar a urgência da necessidade das mesmas.

10 Utilização dos certificados emitidos

Um organismo de controlo acreditado e aprovado pela autoridade de supervisão responsável pela realização de testes de segurança da informação ou de análises das vulnerabilidades pode utilizar certificados ou outros atestados concedidos ao titular da licença de «software» de jogo como parte da sua inspeção. Caso o organismo de controlo utilize certificados existentes como parte da inspeção, deve avaliar se os certificados podem ser considerados provas suficientemente fiáveis da fiabilidade e segurança da informação do sistema de jogo do titular da licença de «software» de jogo.

11 Desvios

O titular da licença é obrigado a comunicar sem demora à autoridade de supervisão quaisquer violações da segurança da informação ou da proteção de dados que detete, se houver motivos para suspeitar que a fiabilidade dos sistemas de jogo ou dos dispositivos de lotaria utilizados pelo titular da licença tenha sido comprometida.

Os titulares de licenças não são obrigados a comunicar incidentes menores de segurança ou de proteção de dados à autoridade de supervisão do jogo, se a eficácia estimada do incidente for de natureza limitada ou se não se considerar que o incidente tenha um impacto significativo na fiabilidade dos sistemas de jogo.

12 Entrada em vigor

O presente regulamento entra em vigor em [dia] de [mês] de 2026.

Serviço Nacional de Polícia
Serviço responsável pelos jogos de fortuna e azar
Konepajankatu 2, PL 50, 11101 Riihimäki
Telefone +358 295 480 181, poliisi.fi