bmm testlabs

Relatório de avaliação para: Gerador de números aleatórios da Diversion en Linea S.A.C RNG Diversion en linea versão 1.1

Fabricante:	**Diversion en Linea S.A.C**
Nome do RNG:	**RNG Diversion en linea versão 1.1**
Número do relatório ATF:	**RNG.BRPR.DVRL.1001.01.01**
Número do documento:	**01**
Data:	**22 de maio de 2025**
Número de páginas:	**8 páginas, incluindo 2 páginas Anexo**

BMM Espanha Testlabs s.l.u.

RELATÓRIO DE AVALIAÇÃO

Nome e endereço do cliente:	Diversion en Linea S.A.C Mza. Bb Lote. 14 Asc. Enatru Peru Chorrillos Lima Peru
Endereçado a:	Lottopar Loterias do Estado do Paraná Rua Marechal Deodoro, 950 - Centro - Curitiba - PR
Número de referência do cliente:	Carta de apresentação do cliente datada de 7 de maio de 2025
Datas dos testes:	Data de início: 7 thde maio de 2025 Data de término: 16 thde maio de 2025
Descrição do produto/jogo:	RNG Diversion en linea versão 1.1 RNG implementado no jogo "Sortida" do Bingo ASSINATURAS: Ver parágrafo 5
Categoria de teste:	Categoria 0
Jurisdições recomendadas:	BRASIL - PARANÁ
Padrão técnico usado para avaliação:	GLI-15 Standards for Electronic Bingo and Keno Systems, versão 1.3, datada de 6 de setembro de 2011
Local onde o teste foi realizado:	BMM Spain Testlabs, s.l.u. Parque Empresarial Vallsolana, Edificio Vinson Camí de Can Camps, 17-19 08174 Sant Cugat del Vallés Barcelona - Espanha
Local onde o relatório foi emitido:	BMM Spain Testlabs, s.l.u.
Conclusão:	Passe
Número de referência da BMM:	DVRL.1001
Método/Procedimentos utilizados:	EURSAM-SPA-MO-41 v.3.1
Consultor(es):	Gianni Piccioni

1. ESCOPO DA AVALIAÇÃO.

A Diversion en Linea S.A.C solicitou à BMM que avaliasse o gerador de números aleatórios (RNG) RNG Diversion en linea em relação aos padrões GLI-15 v1.3:

- GLI-15: Electronic Bingo and Keno Systems v1.3, datado de 6 de setembro de 2011

2. DESCRIÇÃO DO RNG.

O RNG é a função shuffle() do PHP 8.1, que usa o algoritmo Mersenne Twister, juntamente com um roteamento em segundo plano que aumenta a imprevisibilidade do RNG.

3. AVALIAÇÃO BMM REALIZADA.

O BMM examinou o código-fonte do RNG e realizou testes estatísticos na saída do RNG. O(s) arquivo(s) relevante(s) usado(s) está(ão) listado(s) na seção 5.

3.1. REVISÃO DO CÓDIGO-FONTE.

As seções a seguir descrevem a implementação do RNG no código-fonte.

3.1.1 SEMENTE.

A chamada da função shuffle() semeia o RNG automaticamente.

3.1.2 CICLISMO.

O RNG é periodicamente alternado, mesmo quando o jogo está ocioso.

3.1.3 ESCALONAMENTO.

A função shuffle() não introduz nenhuma tendência.

3.1.4 IMPREVISIBILIDADE.

O ciclo de fundo garante maior imprevisibilidade.

3.2. TESTES ESTATÍSTICOS.

Foram realizados testes estatísticos na saída do RNG. A saída bruta do RNG foi submetida a uma série de testes nos conjuntos de testes Empirical, Diehard e NIST. O Apêndice A descreve os testes executados em cada conjunto de testes.

Cada teste testa a hipótese de que o RNG é uma fonte aleatória de números. Um "valor p" é produzido para cada execução de teste, que é a probabilidade de que um processo verdadeiramente aleatório produziria o mesmo resultado ou um resultado mais extremo. Espera-se que os valores de p sejam uniformemente distribuídos entre 0 e 1. Os valores de p de cada teste são avaliados usando um teste de Anderson-Darling. Isso produz um único valor p, que é a probabilidade de que os valores p individuais tenham sido produzidos a partir de uma distribuição uniforme.

Por fim, os valores de p de cada teste no mesmo conjunto de testes são combinados usando o método Holm-Bonferroni para fornecer um valor de p geral. Esse processo ajusta cada valor p para garantir que a probabilidade geral de aceitar o RNG como aleatório corresponda ao intervalo de confiança usado. O valor p geral, igual ao mínimo dos valores p ajustados, é comparado a um valor alfa específico para determinar se o RNG é aceito ou rejeitado como aleatório para um intervalo de confiança específico.

Testes de resistência

Teste	Valores de p	95% de confiança	99% de confiança
Teste de classificação binária 32x32	1,000000	PASS	PASS
Teste de classificação binária 6x8	1,000000	PASS	PASS
Teste de Espaçamento de Aniversário	1,000000	PASS	PASS
Teste de fluxo de bits	1,000000	PASS	PASS
Teste de contagem de 1's	1,000000	PASSE	PASSE
Teste específico Count The 1's	1,000000	PASSE	PASSE
Teste de execução	1,000000	PASSE	PASSE
Teste de compressão	0,290360	PASSE	PASSE
Geral	**0,290360**	**PASSE**	**PASSE**

Conclusão: O RNG é **ACEITO** como aleatório no intervalo de confiança de 95%. Conclusão: O RNG é **ACEITO** como aleatório no intervalo de confiança de 99%.

Testes do NIST

Teste	Valores de p	95% de confiança	99% de confiança
Teste de entropia aproximada	1,000000	PASSE	PASSE
Teste de frequência de bloco	1,000000	PASSE	PASSE
Teste de somas cumulativas	1,000000	PASSE	PASSE
Teste de transformada discreta de Fourier	1,000000	PASSE	PASSE
Teste de frequência	0,904663	PASSE	PASSE
Teste de complexidade linear	1,000000	PASSE	PASSE
Teste de maior duração de um	1,000000	PASSE	PASSE
Teste de correspondências de modelos sem sobreposição	1,000000	PASSE	PASS
Teste de correspondência de modelos sobrepostos	1,000000	PASS	PASS
Teste de excursões aleatórias	1,000000	PASS	PASS
Teste da variante Random Excursions	1,000000	PASS	PASS
Teste de classificação	1,000000	PASS	PASS
Teste de execução	0,887443	PASSE	PASSE
Teste de série	1,000000	PASSE	PASSE
Teste universal	1,000000	PASSE	PASSE
Geral	**0,887443**	**PASSE**	**PASSE**

Conclusão: O RNG é **ACEITO** como aleatório no intervalo de confiança de 95%. Conclusão: O RNG é **ACEITO** como aleatório no intervalo de confiança de 99%.

4. AVALIAÇÃO DOS REQUISITOS TÉCNICOS.

A BMM testou e confirmou a conformidade do RNG com os requisitos técnicos aplicáveis apropriados do RNG do Padrão GLI-15. A BMM realizou os seguintes testes para confirmar a conformidade com as especificações regulatórias relevantes:

Referências	Requisito	Aprovado/Reprovado	Comentário
2. 2.7	**Gerador eletrônico de números aleatórios.**		
2. 2.7.1	Requisitos do gerador de números aleatórios. O uso de um RNG resulta na seleção dos símbolos do jogo ou na produção dos resultados do jogo. A seleção deve:		
2. 2.7.1 a)	Ser estatisticamente independente.	PASS	
Referências	**Requisito**	**Aprovado/Reprovado**	**Comentário**

2. 2.7.1 b)	Conformidade com a distribuição aleatória desejada.	PASSE	
2. 2.7.1 c)	Passar em vários testes estatísticos reconhecidos.	PASSE	
2. 2.7.1 d)	Seja imprevisível.	PASS	
2. 2.7.2	**Testes aplicados.** O laboratório de testes pode empregar o uso de vários testes reconhecidos para determinar se os valores aleatórios produzidos pelo gerador de números aleatórios passam ou não pelo nível de confiança desejado de 95%. Esses testes podem incluir, mas não estão limitados a:		
2. 2.7.2 a)	Teste de qui-quadrado.	N/A	Consulte \Avaliação estatística\Resultados para obter a lista completa de testes
2. 2.7.2 b)	Teste de equidistribuição (frequência).	PASSE	
2. 2.7.2 c)	Teste de lacunas.	N/A	Consulte \Avaliação estatística\Resultados para obter a lista completa de testes
2. 2.7.2 d)	Teste de sobreposições.	N/A	Consulte \Avaliação estatística\Resultados para obter a lista completa de testes
2. 2.7.2 e)	Teste do colecionador de cupons.	PASS	
2. 2.7.2 f)	Teste de permutação.	N/A	Consulte \Avaliação estatística\Resultados para obter a lista completa de testes
2. 2.7.2 g)	Teste de Kolmogorov-Smirnov.	N/A	Consulte \Avaliação estatística\Resultados para obter a lista completa de testes
2. 2.7.2 h)	Testes de critério de adjacência.	N/A	Consulte \Avaliação estatística\Resultados para obter a lista completa de testes
2. 2.7.2 i)	Teste estatístico de ordem.	N/A	Consulte \Avaliação estatística\Resultados para obter a lista completa de testes
2. 2.7.2 j)	Executa testes (os padrões de ocorrências não devem ser recorrentes).	PASSE	
2. 2.7.2 k)	Teste de correlação de interação.	N/A	Consulte \Avaliação estatística\Resultados para obter a lista completa de testes
2. 2.7.2 l)	A potência do teste de correlação serial e o grau de correlação serial (os resultados devem ser independentes do jogo anterior).	PASS	
2. 2.7.2 m)	Testes em subsequências.	PASSE	

Referências	Requisito	Aprovado/Reprovado	Comentário
2. 2.7.3	Requisito de atividade de RNG em segundo plano. O RNG deve ser continuamente alternado em segundo plano entre os jogos e durante o jogo em uma velocidade que não possa ser cronometrada pelo jogador. O laboratório de testes reconhece que, em algum momento durante o jogo, o RNG pode não estar em ciclo quando as interrupções podem ser suspensas. O laboratório de testes reconhece isso, mas deve considerar que essa exceção deve ser mantida em um nível mínimo.	PASS	
2. 2.7.4	Semeadura RNG. A primeira semente será determinada aleatoriamente por um evento não controlado. Após cada sorteio de bola, haverá uma alteração aleatória no processo RNG (nova semente, cronômetro aleatório, atraso, etc.). Isso verificará se o RNG não começa com o mesmo valor todas as vezes. É permitido não usar uma semente aleatória; no entanto, o fabricante deve garantir que os jogos não serão sincronizados.	PASSE	
2. 2.7.6	**Jogos de desenhar bolas.** As consequências para os jogos que representam bolas sendo retiradas de um barril são as seguintes:		
2. 2.7.6 a)	No início de cada jogo, somente as bolas aplicáveis ao jogo devem ser representadas. Para jogos com recursos de bônus e bolas adicionais que são selecionadas, elas devem ser escolhidas a partir da seleção original sem duplicar uma bola já escolhida.	N/A	Jogo de Bingo simples
2. 2.7.6 b)	O barril não poderá ser misturado novamente, exceto conforme previsto nas regras do jogo representado.	N/A	Avaliação de RNG somente
2. 2.7.6 c)	À medida que as bolas são retiradas do tambor, elas devem ser usadas imediatamente, conforme indicado pelas Regras do Jogo. (ou seja, as bolas não devem ser descartadas devido ao comportamento adaptativo do dispositivo de jogo).	N/A	Apenas avaliação de RNG
2. 2.7.7 a)	Se um número aleatório com um intervalo menor do que o fornecido pelo RNG for necessário para alguma finalidade dentro do dispositivo de jogo, o método de redimensionamento (ou seja, a conversão do número para o intervalo inferior) deve ser projetado de forma que todos os números dentro do intervalo inferior sejam convertidos em números aleatórios. são igualmente prováveis.	N/A	Somente o método de embaralhamento de bolas é aplicado.
2. 2.7.7 b)	Se um determinado número aleatório selecionado estiver fora do intervalo de distribuição igual dos valores de redimensionamento, é permitido descartar esse número aleatório e selecionar o próximo na sequência para fins de redimensionamento.	N/A	Somente o método de embaralhamento de bolas é aplicado.

2. 2.8	Requisitos do gerador mecânico de números aleatórios.		
Referências	**Requisito**	**Aprovado/Reprovado**	**Comentário**
2. 2.8.1	**Jogos RNG baseados em mecânica.** Os jogos RNG baseados em mecânica são jogos que usam as leis da física para gerar o resultado do jogo. Todos os jogos RNG de base mecânica devem atender aos requisitos deste documento, com exceção dos requisitos para geradores eletrônicos de números aleatórios. Além disso, os jogos RNG baseados em mecânica devem atender às seguintes regras:		
2. 2.8.1 a)	O laboratório de testes testará várias iterações por meio de comunicações via PC para coletar dados suficientes para verificar a aleatoriedade. Além disso, o fabricante pode fornecer dados em tempo real para ajudar nessa avaliação.	N/A	Apenas avaliação do software RNG
2. 2.8.1 b)	As peças mecânicas devem ser construídas com materiais que impeçam a decomposição de qualquer componente ao longo do tempo. (por exemplo, uma bola não deve desintegrar).	N/A	Apenas avaliação do software RNG
2. 2.8.1 c)	As propriedades dos itens físicos usados para escolher a seleção não devem ser alteradas.	N/A	Apenas avaliação do software RNG
2. 2.8.1 d)	O jogador não deve ter a capacidade de interagir fisicamente, entrar em contato físico ou manipular a máquina fisicamente com o parte mecânica do jogo.	N/A	Apenas avaliação do software RNG
2. 2.8.2	**Método de mistura por esferas mecânicas.** Um dispositivo mecânico que use fluxo de ar para misturar e retirar bolas aleatoriamente para determinar as letras e números ou símbolos a serem chamados deve ser utilizado em locais que não usem RNGs eletrônicos para sortear as bolas vencedoras. Esse dispositivo deve ser construído da seguinte maneira:		
2. 2.8.2 a)	Isso permitirá que os participantes tenham uma visão completa da ação de mistura das bolas.	N/A	Apenas avaliação do software RNG
2. 2.8.2 b)	A operação não pode ser interrompida para alterar o posicionamento aleatório das bolas no receptáculo de saída do dispositivo, exceto quando o dispositivo é desligado.	N/A	Apenas avaliação do software RNG
2. 2.8.3	**Bolas de bingo.** Um conjunto de bolas, cada uma com um número exclusivo e as letras B, I, N, G ou O, desde que as letras B, I, N, G ou O não precisem aparecer se as bolas forem usadas para jogos de bingo de velocidade ou de face oculta. Os seguintes requisitos adicionais relativos às bolas de bingo devem ser atendidos:		
2. 2.8.3 a)	Todo o conjunto de bolas deverá estar disponível para inspeção pelos jogadores antes do início de uma sessão de bingo para determinar se todas estão presentes e em condição operacional.	N/A	Apenas avaliação do software RNG

2. 2.8.3 b)	Cada bola numerada deve ter o mesmo peso que as outras bolas e estar livre de defeitos.	N/A	Apenas avaliação do software RNG
2. 2.8.3 c)	Cada conjunto de bolas em jogo deve ser distinguível de todos os outros conjuntos de bolas. bolas em jogo.	N/A	Software RNG Somente avaliação
Referências	**Requisito**	**Aprovado/Reprovado**	**Comentário**
2. 2.8.4	Resultado do RNG. Deverá haver um método para exibir o resultado do RNG para os números chamados em todos os jogos de bingo. O visor deve estar visível para todos os jogadores e indicar claramente todos os números que foram chamados.	N/A	Apenas avaliação do software RNG

5. ARQUIVOS DE CÓDIGO-FONTE.

O(s) arquivo(s) a seguir é(são) usado(s) pelo RNG. As assinaturas fornecidas são geradas usando SHA1.

Arquivos	SHA1
Kernel.php	1BAD0C9B2B64AE526E18FF28A72377F975B00679
RNG_cycler.php	9B66A2113DD35F7CEEC5458087713785E650A864
SortearCommand.php	A6AFEF5D192499DE4B4ECFEA37E6548765163EE4
SorteioAutomatico.php	C2B0A7DADDF9285BB303B5574B817784020FCD77
SorteioService.php	C23C27297BC0CEB132726965F44741DD021E6352

6. INFORMAÇÕES/OBSERVAÇÕES ADICIONAIS.

N/A.

7. CONCLUSÃO.

De acordo com os resultados do teste[1], a BMM Spain Testlabs s.l.u. confirma que o item enviado para teste está em conformidade com todos os regulamentos relevantes listados na seção Escopo da avaliação.

Atenciosamente,

30378334A
RUBÉN BAPTISTA
(C:B64622251)

Firmado digitalmente por 30378334A RUBÉN BAPTISTA (C:B64622251)
Fecha: 2025.05.22 13:16:29 +02'00'

Vice-Presidente Sênior de Operações da EURSAM
Rubén Baptista

1Os resultados incluídos neste documento referem-se exclusivamente à amostra testada, conforme descrito n a seção correspondente.

APÊNDICE A TESTES ESTATÍSTICOS

Os testes a seguir foram usados para testar as propriedades estatísticas do RNG.

Testes de resistência

Os testes Diehard são baseados no conjunto de testes publicado por George Marsaglia em 1995. Eles testam sequências de saída binária bruta do RNG.

Teste de classificação binária 32x32	As matrizes são criadas usando 32 palavras de 32 bits. As classificações das matrizes resultantes são contadas.
Teste de classificação binária 6x8	Igual ao teste de classificação binária 32x32, exceto pelo fato de que cada matriz é formada usando 6 valores, cada um deles pegando 8 bits de palavras sucessivas de 32 bits com um deslocamento específico. Todos os os possíveis deslocamentos são testados separadamente.
Teste de Espaçamento de Aniversário	Os valores de 26 bits são obtidos de palavras sucessivas de 32 bits com um deslocamento específico. Os valores são classificados e os espaçamentos entre eles são calculados. O número de espaçamentos do mesmo tamanho são contados. Todos os deslocamentos possíveis são testados separadamente.
Teste de fluxo de bits	Os blocos de 2^18 valores são tratados como um fluxo de valores de 20 bits sobrepostos. O número de valores possíveis de 20 bits que não são encontrados em cada bloco é contado.
Teste de contagem de 1's	Os valores de 8 bits são obtidos e recebem uma "letra" com base no número de que aparecem na representação binária de cada valor. Grupos sobrepostos de 5 "letras" são contadas.
Teste específico Count The 1's	Semelhante ao teste Count The 1's Stream, exceto que os valores de 8 bits são obtidos de palavras sucessivas de 32 bits com um deslocamento específico. Todos os deslocamentos possíveis são testados separadamente.
Teste de execução	Conta sequências de palavras de 32 bits crescentes e decrescentes. Observe que esse é um teste diferente do teste de execução nos testes empírico e NIST.
Teste de compressão	Um valor de 2^31 é multiplicado repetidamente por palavras de 32 bits, dividindo por 2^32 e obtendo o teto do resultado a cada vez. O número de palavras sucessivas necessárias para reduzir o valor a 1 é contado. O valor é redefinido para 2^31 e o processo é repetido.

Testes do NIST

Os testes do NIST baseiam-se no conjunto de testes lançados pelo National Institute of Standards and Technology na Publicação Especial 800-22, Revisão 1a (revisada em abril de 2010). Eles testam sequências de saída binária bruta do RNG.

Teste de entropia aproximada	Semelhante ao teste serial, conta cada valor possível de m bits, mas faz isso para dois comprimentos de m bits adjacentes e compara os dois.
Teste de frequência de bloco	Semelhante ao teste de frequência, exceto que os dados são divididos em blocos de tamanho igual. O número de uns e zeros em cada bloco é contado.
Teste de somas cumulativas	Os passeios aleatórios são criados convertendo os dados em +1 / -1 para 1 / 0, respectivamente, e somando os valores consecutivos.
Teste de transformação discreta de Fourier	Os dados são transformados usando uma Transformada Discreta de Fourier. O número de picos dentro do limite de 95% é contados.
Teste de frequência	O número de uns e zeros na saída binária é contados.
Teste de complexidade linear	O comprimento da complexidade linear da sequência aleatória é determinado.

Teste de maior duração de um	Os dados são divididos em blocos de tamanho igual. A sequência mais longa de uns em cada bloco é determinada e contada.
Teste de correspondências de modelos sem sobreposição	Os dados são divididos em blocos de tamanho igual. Cada bloco é pesquisado em busca de um padrão específico de bits e contado. Um teste separado é executado para vários padrões de bits. Cada padrão de bits pesquisado não se sobrepõe a si mesmo. Ou seja, quando o padrão é correspondido, o final do padrão não pode ser o início de outra partida.
Teste de correspondência de modelos sobrepostos	Semelhante ao Non-Overlapping Template Matchings Test, exceto que apenas um padrão é pesquisado, que pode se sobrepor com ele mesmo.
Teste de excursões aleatórias	Assim como no teste de somas cumulativas, os passeios aleatórios são criados convertendo os dados em +1 / -1 para 1 / 0, respectivamente, e somando os valores consecutivos. O número de vezes que um determinado estado é visitado entre os retornos a zero é contado. Testes separados são executados para vários estados de -4 a +4, não incluindo 0.
Teste da variante Random Excursions	Semelhante ao teste de excursões aleatórias, exceto que o número de vezes que um determinado estado é visitado é contado para toda a sequência. Testes separados são executados para vários estados de -9 a +9, não incluindo 0.
Teste de classificação	As matrizes são criadas usando 32 palavras de 32 bits. As classificações das matrizes resultantes são contadas. Observe que esse é fundamentalmente o mesmo teste que o teste de classificação binária 32x32 nos testes Diehard, embora a implementação possa ser diferente. diferente.
Teste de execução	Sequências de bits consecutivos com o mesmo valor de vários são contados.
Teste de série	Contagens de cada valor possível de m-bit. Testes separados são executados para vários comprimentos de m bits.