World Lottery Association

WLA-SCS:2024

WLA - Estándar de control de seguridad

Requisitos de seguridad e integridad de la información para operadores de loterías, videoloterías, apuestas deportivas y de deportes electrónicos, asi como también para sus proveedores.

Índice

Preámbulo 2

Introducción 3

1. Alcance 3

2. Referencias normativas 4

3. Términos y definiciones 4

3.1 Abreviaturas 4

3.2 Definiciones 4

4. Visión general 4

5. Obligaciones generales de gestión de la seguridad y la integridad 5

5.1 Sistema de gestión de la seguridad de la información (ISMS) 5

5.2 Alcance del ISMS 5

5.3 Declaración de aplicabilidad 5

Anexo A (controles «G»): Controles organizacionales 6

Anexo B (controles «L»): Controles para la operación de juegos 11

Anexo C (controles «S»): Controles para el desarrollo de sistemas de juego y la prestación de servicios de juegos 20

Anexo D (controles «M»): Controles para juegos multijurisdiccionales 23

Preámbulo

La Asociación Mundial de Loterías (WLA, por sus siglas en inglés) reconoce desde su fundación la necesidad de que los operadores de loterías, videoloterías, apuestas deportivas y de deportes electrónicos (en lo sucesivo denominados « operadores de juegos ») dispongan de un estándar de seguridad e integridad adecuado, motivo por el cual ha seguido adelante con el trabajo iniciado por sus predecesores.

Los operadores de juegos tienen la necesidad empresarial de desarrollar entornos que mantengan una posición de seguridad e integridad visible y documentada para retener la confianza tanto de los jugadores como de las partes interesadas. El Estándar de control de seguridad de la WLA (WLA-SCS, por sus siglas en inglés) tiene por objeto ayudar a los operadores de juegos de todo el mundo, y a sus proveedores, a alcanzar niveles de control acordes con las prácticas de seguridad y calidad de la información generalmente aceptadas, así como con las obligaciones específicas de la industria, permitiéndoles reforzar la confianza en la integridad de sus operaciones. La certificación en el estándar WLA-SCS ofrece una medida objetiva respecto del desempeño del operador de juegos en materia de control de seguridad y gestión de riesgos.

El Comité de Seguridad y Gestión de Riesgos de la WLA (WLA SRMC, por sus siglas en inglés) elaboró el estándar WLA-SCS. Este comité está conformado por representantes y especialistas en seguridad de los operadores de juegos de todo el mundo. Al comparar las prácticas actuales en materia de seguridad e integridad con las prácticas aprobadas por los expertos en juegos de todo el mundo, se logró crear un marco sólido de seguridad y gestión de riesgos para los operadores de juegos y sus proveedores.

El Comité de Seguridad y Gestión de Riesgos de la WLA revisa todas las normas de control de seguridad para su uso en el sector de los juegos y sirve de referencia para el sector en temas de seguridad y gestión de riesgos. Supervisa el proceso de certificación en el estándar WLA-SCS, mediante el cual se verifica el cumplimiento de los miembros y de los miembros asociados de la WLA con el estándar.

Todos los estándares del comité, nuevos o actualizados, deben ser respaldados y emitidos por el Comité Ejecutivo de la WLA y autorizados por los delegados presentes en la Asamblea General bienal antes de su publicación.

La estructura de este estándar responde a la que establece la Organización Internacional de Normalización (ISO, por sus siglas en inglés) y la WLA tiene un firme compromiso de mantenerlo actualizado y adaptado en concordancia la norma ISO/IEC 27001.

Introducción

El presente estándar define la norma en materia de seguridad, integridad y gestión de riesgos que debe aplicar el sector de los juegos; y se pretende sea considerado como referencia para el sector en cuestiones de seguridad e integridad. Se describe aquí un proceso de gestión de la seguridad conforme con normas reconocidas a escala internacional y con normas básicas de seguridad que representan buenas prácticas para los operadores de juegos. El estándar incluye un conjunto integral de controles y obligaciones para los operadores de juegos y sus proveedores.

El estándar WLA-SCS puede considerarse como la base para construir relaciones de confianza con las partes interesadas y los reguladores de la industria con el fin de llevar a cabo operaciones de juegos o juegos multijurisdiccionales; también puede ser una importante ayuda para la alta dirección, ya que proporciona una revisión independiente para fomentar una mayor confianza en la seguridad de las operaciones de juegos.

La más reciente versión del estándar, WLA-SCS:2024, presenta un marco de certificación con dos niveles.

El cumplimiento con el Nivel 1 del estándar WLA-SCS confirma que el operador de juegos tiene un nivel básico pero esencial en materia de seguridad de la información y demuestra su compromiso de alcanzar el más alto nivel de certificación en el estándar, el Nivel 2. La certificación en el Nivel 1 es ideal para aquellas organizaciones miembro de la WLA que prefieren un enfoque gradual para la certificación.

Por su parte, el cumplimiento con el Nivel 2 permite a las organizaciones miembro de la WLA garantizar la integridad, la disponibilidad y la confidencialidad de los servicios y de los datos esenciales para un funcionamiento seguro. Gracias a la conjugación de la evaluación de los controles para operadores de juegos y del cumplimiento con la norma ISO/IEC 27001 para los Sistemas de Gestión de la Seguridad de la Información, el Nivel 2 del estándar representa el estándar de certificación más completo y extenso disponible tanto para los operadores de juegos como para sus proveedores.

La adopción del estándar WLA-SCS supone una decisión estratégica. Inciden en la concepción y aplicación de los sistemas de gestión de seguridad e integridad de una organización sus necesidades, objetivos, riesgos y requisitos de seguridad específicos, así como los procesos empleados, la dimensión y la estructura de la organización. Se espera que estos factores y sus sistemas de soporte cambien con el tiempo y, además, es de esperar que la adopción de un sistema de gestión se adapte a las necesidades de la organización, por ejemplo, una situación sencilla requiere un sistema sencillo.

Las partes interesadas internas y externas podrán utilizar el cumplimiento con el estándar WLA-SCS para evaluar la seguridad e integridad de los sistemas de un operador de juegos y de sus proveedores.

Además de ajustarse a la norma ISO/IEC 27001, el estándar WLA-SCS se conforma a lo estipulado en la norma ISO 9001 para permitir una aplicación y un funcionamiento sistemáticos e integrales junto con otros estándares de gestión conexos.

1. Alcance

El estándar WLA-SCS abarca todo tipo de operaciones de juegos, incluidas empresas comerciales, organismos públicos y organizaciones sin ánimo de lucro.

El estándar especifica los requisitos para definir, aplicar, explotar, controlar, revisar, mantener y mejorar un sistema documentado de seguridad e integridad en el marco general de riesgos de la organización.

Los requisitos previstos en el estándar son genéricos y tienen como fin resultar aplicables a todas las organizaciones, independientemente del tipo, de la dimensión o de la naturaleza de la organización. En cualquier caso, no se podrá excluir ninguno de los controles previstos en los Anexos A, B, C o D, salvo con la autorización formal de la WLA.

Cualquier exclusión de los controles previstos en los Anexos A, B, C o D deberá justificarse formalmente y se deberá presentar evidencia de que las personas responsables han autorizado tales exclusiones. En los casos en que algún control se excluya, no se aceptarán declaraciones de conformidad con el estándar, salvo que tales exclusiones no afecten a la capacidad o la responsabilidad de las organizaciones de ofrecer seguridad e integridad conformes con los requisitos que determine una evaluación de riesgos y se prevean en las leyes o los reglamentos aplicables. En el alcance de la certificación descrito en el certificado WLA-SCS, se anotará cualquier control de los Anexos A, B, C o D que se hubiere excluido.

Nota: Si una organización dispone ya de un sistema de gestión de procesos empresariales operativo (por ejemplo, en relación con las normas ISO 9001 o ISO 14001), en la mayoría de los casos es recomendable satisfacer las obligaciones previstas en el estándar WLA-SCS en el seno del sistema de gestión existente.

Importante: El estándar no pretende incluir todas las estipulaciones necesarias de un contrato. Los miembros de la WLA que adopten el estándar WLA-SCS son responsables de su correcta aplicación. El cumplimiento de cualquier estándar no exime *per se* del cumplimiento de cualquier obligación legal.

2. Referencias normativas

En este estándar, se hace referencia a los siguientes documentos de manera normativa y son indispensables para su aplicación. Para las referencias con fecha, se aplica únicamente la edición citada. Para las referencias sin fecha, se aplica la edición más reciente del documento citado, incluidas las enmiendas.

ISO/IEC 27001:2022 Seguridad de la información, ciberseguridad y protección de la privacidad - Sistemas de gestión de la seguridad de la información – Requisitos. Se aplica la edición actual (2022) o la edición más reciente.

WLA-SCS:2024 Código de prácticas – directrices de mejores prácticas para los controles y las obligaciones de seguridad e integridad del estándar WLA-SCS.

Guía de certificación en el estándar WLA-SCS.

3. Términos y definiciones

3.1 Abreviaturas

WLA: World Lottery Association (Asociación Mundial de Loterías)

WLA-SCS: Estándar de control de seguridad de la WLA

CSGR: Comité de Seguridad y Gestión de Riesgos

3.2 Definiciones

En este apartado, se recogen únicamente aquellos términos que se utilizan con un significado específico a lo largo del estándar. La mayoría de los términos que aquí se emplean se utilizan de acuerdo con sus definiciones aceptadas en diccionarios o con definiciones habitualmente aceptadas que pueden consultarse en glosarios de seguridad de la ISO u otros compendios reconocidos de términos de seguridad.

Activos: información o recursos que proteger mediante contramedidas.

Personal: deberá interpretarse como cualquier empleado, contratista u otro tercero que trabaja para el operador de juegos o el proveedor de juegos, y que, por su función o acceso, tiene el potencial de afectar a la confidencialidad, disponibilidad o integridad del juego.

Sistema de juego: deberá interpretarse como todos o cualquier subconjunto de recursos tecnológicos e informativos que permiten la oferta de un juego.

Servicios de juego: cualquier tipo de sistema de juego que se ofrece como servicio.

Proveedor de juegos: se refiere a las entidades que ofrecen sistemas de juego o servicios de juegos.

Operador de juegos: se refiere a las entidades que operan juegos.

Organización: se refiere al operador o proveedor de juegos objeto de certificación bajo este estándar.

4. Visión general

El objetivo principal del enfoque de seguridad e integridad que ofrecemos a las organizaciones miembro de la WLA es garantizar un funcionamiento adecuado y ofrecer confianza.

La confianza en una operación de juegos es clave para conservar a los jugadores y a las demás partes interesadas. Por tanto, las organizaciones miembro de la WLA deben desarrollar y mantener un entorno de seguridad visible y documentado.

El CSGR de la WLA describe en el estándar WLA-SCS las obligaciones, los objetivos de control y los controles que se consideran mejores prácticas. Una organización miembro de la WLA dispondrá de un sistema de gestión de seguridad de la información conforme con todos los requisitos previstos en la norma ISO/IEC 27001, así como con las obligaciones y los controles obligatorios de este estándar.

El estándar WLA-SCS incorpora obligaciones y controles de base en los procesos generales de seguridad, integridad y gestión de riesgos del operador de juegos, evitando interferencias con marcos de seguridad más generales. Ofrece a los profesionales de la seguridad e integridad de los juegos un proceso mediante el cual pueden gestionar formalmente, actualizar y mejorar sus controles de manera continua. Por tanto, los operadores de juegos deben desarrollar y mantener un entorno de seguridad visible y documentado.

El estándar WLA-SCS comprende cuatro partes en las que se especifican los controles mínimos necesarios para la gestión eficaz de la seguridad e integridad de los operadores y proveedores de juegos a la industria.

La primera parte (Anexo A – Controles «G»: controles organizacionales) incluye el cumplimiento con la norma ISO/IEC 27001 dentro de un enfoque global, además de 30 controles básicos adicionales de la WLA.

La segunda parte (Anexo B – Controles «L»: controles para la operación de juegos) proporciona 62 controles adicionales de seguridad e integridad específicos al sector de los juegos, que representan las mejores prácticas actuales.

La tercera parte (Anexo C – Controles «S»: controles para el desarrollo de sistemas de juego y la prestación de servicios de juegos) contiene 21 controles basados en productos y servicios que ofrecen los operadores y proveedores de loterías, videoloterías, apuestas deportivas y deportes electrónicos y otros juegos que desarrollan y gestionan sus propios sistemas y servicios de juegos.

La cuarta parte (Anexo D – Controles «M»: controles para juegos multijurisdiccionales) comprende 11 controles requeridos para participar en juegos administrados por la Asociación Multiestatal de Loterías de los Estados Unidos (MUSL, por sus siglas en inglés).

5. Obligaciones generales de gestión de seguridad e integridad

5.1 Sistema de gestión de la seguridad de la información (SGSI)

Las organizaciones que deseen certificarse en el Nivel 2 del estándar WLA-SCS:2024 deben contar con un sistema de gestión de la seguridad de la información que se ajuste a los requisitos previstos en la norma ISO/IEC 27001.

5.2 Alcance del SGSI

El SGSI de la organización abarcará todas las actividades de sus operaciones relacionadas con los juegos, incluidos todos los activos y los sistemas de información conexos. Su alcance podrá excluir únicamente aquellas operaciones de la organización ajenas a actividades de juegos. Deberán identificarse todas las operaciones excluidas, así como detallarse las causas de exclusión. Las funciones organizativas generales (por ejemplo, recursos humanos, planificación y finanzas) necesarias para las operaciones de loterías, videoloterías, apuestas deportivas y de deportes electrónicos se encuentran incluidas en el alcance del SGSI.

5.3 Declaración de aplicabilidad

La declaración de aplicabilidad del SGSI de la organización debe incluir expresamente todos los controles previstos en los Anexos A, B, C y D del estándar WLA-SCS. Las declaraciones de inaplicabilidad deberán justificarse detalladamente y la WLA deberá autorizarlas formalmente.

Anexo A (controles «G»): Controles organizacionales

G.1 Organización de seguridad

G.1.1 Asignación de responsabilidades de seguridad

Objetivo: Garantizar la adopción eficaz de las responsabilidades de la función de seguridad.

G.1.1.1	Foro de seguridad	*Control* Se creará formalmente un foro de seguridad u otra estructura organizativa formada por miembros de la alta dirección con el fin de seguir y evaluar el SGSI y garantizar que resulte en todo momento idóneo, adecuado y eficaz; deberán redactarse actas formales de las reuniones, que deberán celebrarse al menos cada seis meses.
G.1.1.2	Función de seguridad	*Control* Existirá una función de seguridad que se encargará de elaborar una estrategia de seguridad acorde a la organización en general. Esta función de seguridad trabajará posteriormente con las otras divisiones de la organización para aplicar los planes de acción conexos; participará en la revisión de todas las labores y todos los procesos necesarios en materia de seguridad de la organización, incluida, pero sin limitarse a, la protección de la información y de los datos, de las comunicaciones, de la infraestructura física y virtual, del personal y de la seguridad operativa de la organización en general.
G.1.1.3	Provisión de información de la función de seguridad	*Control* La función de seguridad dará cuentas, al menos, a la dirección ejecutiva sin circunscribirse a la función de tecnología en lo referente a la gestión de seguridad de riesgos.
G.1.1.4	Posición de la función de seguridad	*Control* Dispondrá de las competencias y las facultades suficientes, y tendrá acceso a todos los recursos necesarios para permitir la adecuada evaluación, gestión y reducción de riesgos.
G.1.1.5	Responsabilidad de la función de seguridad	*Control* El responsable de la función de seguridad será un miembro de pleno derecho del foro de seguridad y será responsable de recomendar políticas de seguridad y modificaciones.

G.2 Seguridad de recursos humanos

G.2.1 Adopción de un código de conducta

Objetivo: Garantizar la efectiva adopción de un código de conducta adecuado.

G.2.1.1	Código de conducta	*Control* Se facilitará un código de conducta a todo el personal al momento de su contratación. Todo el personal reconocerá formalmente la aceptación de este código.
G.2.1.2	Cumplimiento y medidas disciplinarias	*Control* El código de conducta incluirá declaraciones de cumplimiento de todos los procedimientos y las políticas y de que su infracción u otros incumplimientos del código podrían traducirse en medidas disciplinarias.
G.2.1.3	Conflictos de intereses	*Control* El código de conducta deberá obligar al personal a comunicar los conflictos de intereses relacionados con su relación contractual según se produzcan. Se citarán en el código ejemplos concretos de conflictos de intereses.
G.2.1.4	Hospitalidad u obsequios	*Control* El código de conducta incluirá disposiciones contra la corrupción, que abarcarán las atenciones de hospitalidad y los obsequios que se reciban de o que se les ofrezcan a personas o entidades con las que la organización mantiene una relación comercial.
G.2.1.5	Política corporativa sobre las apuestas	*Control* Se elaborará una política interna, conforme a las obligaciones legislativas y reglamentarias, donde se aborde el derecho a jugar del personal y sus dependientes. No podrán jugar aquellas personas cuyas funciones pudieran afectar la integridad de los juegos sin connivencia. En los casos en los que la política contemple una prohibición de juego, se definirán explícitamente las funciones a las que atañe tal prohibición y se hará cumplir mediante contrato con el personal o su empleador (si no se trata del mismo operador o proveedor de juegos).
G.2.1.6	Seguridad del personal	*Control* Se definirá una política y un proceso que, mediante un estudio de seguridad, permita poner la confianza en las personas que pudieran afectar la integridad de los juegos. Se definirá también una política y un proceso asociados para supervisar las actividades del personal en el sistema a fin de detectar e investigar cualquier actividad que pudiera afectar la integridad del juego. Estas políticas garantizarán un equilibrio entre el derecho de cada persona a la privacidad y la obligación de la organización de proteger la integridad de los juegos.
G.2.1.7	Separación de responsabilidades	*Control* Se definirá una política de separación de funciones que describa las funciones y responsabilidades respectivas de las personas a cargo de los procesos críticos que pudieran afectar la integridad de un juego, por ejemplo, el procesamiento de los sorteos y el pago de premios, entre otros, con la finalidad de evitar posibles connivencias. Además, ningún grupo o equipo tendrá control general que le permitiera afectar la integridad del juego sin la supervisión de la dirección.
G.2.1.8	Política sobre la protección del personal	*Control* Se definirá una política para garantizar que el personal que trabaja solo, el que trabaja fuera de las instalaciones de la organización o dentro de ellas en un área de acceso público, reciba un nivel adecuado de protección para su seguridad e integridad física.

G.3 Seguridad física y medioambiental

G.3.1 Zonas seguras

Objetivo: Garantizar la seguridad del acceso a centros de datos de juegos en producción u otras áreas de los sistemas importantes para las operaciones de juegos.

G.3.1.1	Control de acceso físico	*Control* El acceso físico a centros de datos de sistemas de juegos en producción salas de ordenadores, centros de operaciones en red y otras áreas críticas definidas deberá restringirse y deberá disponerse de personal para resguardar y supervisar la zona en todo momento. Aunque se trata de un acceso basado en riesgo, en la práctica requerirá un mínimo de un proceso auditable de autentificación de doble factor. Se documentará la lista de áreas críticas.

G.4 Control de acceso a sistemas de juego

G.4.1 Gestión del acceso a usuarios

Objetivo: Garantizar el acceso a usuarios autorizados y evitar el acceso no autorizado a los sistemas de juego.
Para los proveedores de juegos se deberán aplicar los controles descritos en la sección G.4 a los repositorios de códigos empleados para desarrollar sistemas de juego.

G.4.1.1	Funciones de acceso de usuarios	*Control* La gama de funciones disponibles para el usuario se definirá y mantendrá junto con el responsable del proceso, la función de TI y la función de seguridad.
G.4.1.2	Registro de acceso de usuarios	*Control* Se registrarán todas las actuaciones que se lleven a cabo en los sistemas de juego, sea por cuentas de usuarios o del sistema, y tales registros se supervisarán, se revisarán con regularidad y se tomarán medidas al respecto, de ser necesario.

G.5 Seguridad de los sistemas de información

G.5.1 Controles criptográficos

Objetivo: Proteger por medios criptográficos la confidencialidad, la autenticidad y la integridad de las claves criptográficas y de los datos importantes relacionados con los juegos y los clientes.

G.5.1.1	Controles criptográficos para la confidencialidad e integridad de los datos en reposo en sistemas portátiles y terminales	*Control* Se cifrará la información sensible almacenada en sistemas informáticos portátiles para proteger la confidencialidad e integridad de la información sensible en reposo en los terminales.
G.5.1.2	Controles criptográficos para la confidencialidad e integridad de los datos en tránsito por redes	*Control* Para proteger la confidencialidad e integridad de la información, según corresponda, se cifrará la información sensible que se transmita por redes que, según evidencien los análisis de riesgos, carezcan de niveles de protección adecuados.

		Se incluye aquí, entre otros, los datos de validación y toda información relevante relacionada con los juegos, los clientes y las transacciones financieras.
G.5.1.3	Controles criptográficos para la integridad de la información sensible en boletos	*Control* Se aplicarán controles criptográficos para la integridad de los datos de boletos ganadores que se almacenen y la información de validación. Se aplicará este control a todos los tipos de juego.

G.5.2 Prueba del sistema *Objetivo:* Habilitar y realizar pruebas del sistema.		
G.5.2.1	Política sobre la metodología de las pruebas	*Control* La política sobre la metodología de las pruebas incluirá estipulaciones orientadas a evitar el uso de datos creados en un sistema de producción activo para el período del sorteo en curso y prevenir la utilización de datos personales de los jugadores, de los minoristas o del personal. En este contexto, se entenderá por período del sorteo en curso como el lapso durante el cual se pueden reclamar premios.
G.5.2.2	Pruebas de seguridad en el sistema de juego	*Control* Se realizarán pruebas exhaustivas en la función de seguridad del sistema de juego antes del uso del entorno de producción y cuando se hayan realizado cambios significativos.

G.5.3 Seguridad de los servicios gestionados por terceros *Objetivo:* Garantizar la seguridad de la información de los sistemas de juego y sus componentes que son gestionados por terceros u hospedados en la nube.		
G.5.3.1	Cumplimiento de la norma ISO 27001	*Control* Los entornos gestionados (incluidos los servicios en la nube, los servicios hospedados y en general todos los servicios gestionados) que operan los sistemas de juego y los componentes del sistema de juego deberán cumplir con la norma ISO/IEC27001. Un entorno gestionado se define como los recursos informáticos gestionados por terceros a los que una organización se suscribe por servicios.
G.5.3.2	Responsabilidades y procedimientos documentados	*Control* Los siguientes elementos deberán documentarse, comunicarse e implementarse: • responsabilidades de roles de seguridad de la información compartidas entre la organización y el proveedor de servicios gestionados • procedimientos para las operaciones administrativas en el entorno de servicios gestionados y su supervisión • un proceso de finalización que abarque la devolución y eliminación de los activos de la organización de manera oportuna.
G.5.3.3	Segregación y control de acceso	*Control* Se protegerá el entorno virtual del servicio gestionado de la organización de otros clientes con servicio de hospedaje y de personas no autorizadas.

G.5.3.4	Fortalecimiento y protección de los componentes virtuales	*Control* Se fortalecerán y protegerán los componentes virtuales en el entorno del servicio gestionado. Se verificará la consistencia de las configuraciones entre las redes físicas y virtuales conforme a la política de seguridad de red del proveedor del servicio gestionado.
G.5.3.5	Supervisión	*Control* La organización podrá supervisar aspectos específicos del funcionamiento del servicio gestionado que utiliza.

G.5.4 Seguridad del sistema de juego

Objetivo: Proteger la confidencialidad, integridad y disponibilidad de los sistemas de juego con el objetivo de proteger los juegos y los datos de los jugadores.

G.5.4.1	Arquitectura de sistemas por capas	*Control* La organización deberá implementar una arquitectura de seguridad por capas dentro de los sistemas de juego a fin de garantizar la seguridad en el almacenamiento y tratamiento de datos.
G.5.4.2	Divulgación responsable	*Control* La organización contará con una Política de divulgación responsable para la divulgación de las vulnerabilidades de seguridad por parte del público al operador de juegos.

G.6 Disponibilidad del sistema y continuidad del negocio

G.6.1 Disponibilidad de los servicios y continuidad del negocio

Objetivo: Garantizar la protección de la imagen y la reputación de la organización y contrarrestar las posibles interrupciones de la actividad empresarial.

G.6.1.1	Obligaciones de disponibilidad y resiliencia	*Control* La organización documentará la lista de servicios críticos para los jugadores (tanto minoristas como canales digitales) necesarios para el funcionamiento continuo de los juegos, así como las obligaciones de disponibilidad y resiliencia de dichos servicios. Los sistemas se diseñarán conforme a esas obligaciones.
G.6.1.2	Continuidad del negocio	*Control* La organización preparará un plan de continuidad del negocio documentado que abarque, como mínimo, el funcionamiento continuo de los juegos y la confianza continua de las partes interesadas en la integridad de las operaciones de juego. Además, la organización planificará, ejecutará y evaluará ejercicios de continuidad empresarial en intervalos regulares a fin de preparar a la organización para situaciones de crisis, que incluya los elementos descritos en el plan de continuidad del negocio.

Anexo B (controles «L»):
Controles para la operación de juegos

L.1 Boletos físicos para juegos instantáneos

L.1.1 Funcionamientos de los juegos instantáneos

Objetivo: Garantizar que los diseños y la producción de los juegos cumplan los requisitos legales y normativos; garantizar la integridad del juego y prevenir el fraude.

L.1.1.1	Gestión del ciclo de vida y requisitos de integridad	*Control* La organización documentará un procedimiento en el que especifique los requisitos de integridad para cada juego instantáneo durante todo el ciclo de vida del juego, desde su diseño hasta su destrucción.
L.1.1.2	Integridad de los datos del juego	*Control* Se establecerán controles para garantizar la integridad de los datos del juego que abarcarán, entre otros, la importación de los datos del juego al sistema de juego y la transferencia de los datos de validación entre el proveedor, el operador y los minoristas.
L.1.1.3	Confidencialidad sobre el boleto ganador	*Control* Se establecerán controles para garantizar que, antes de que se reclame el premio, ninguna persona en la organización tenga acceso o conocimiento alguno de cuál boleto instantáneo es ganador y cuál no; tampoco podrán identificar el lugar donde se encuentra el boleto ganador ni a cuál minorista le fue asignado.

L.2 Sorteos de lotería

L.2.1 Gestión de sorteos de lotería

Objetivo: Garantizar que los sorteos se realicen a las horas que exija el reglamento y de acuerdo con las normas del juego de lotería de que se trate.

L.2.1.1	Celebración del sorteo	*Control* Se definirá una política para garantizar que los sorteos de lotería se realicen en el marco de actos planificados y controlados y de acuerdo con instrucciones de funcionamiento claras.
L.2.1.2	Instrucciones de funcionamiento de sorteos	*Control* La organización publicará instrucciones de funcionamiento antes de los sorteos, incluidas instrucciones específicas para cada uno de ellos.
L.2.1.3	Miembros del equipo del sorteo	*Control* Las instrucciones de funcionamiento definirán la composición del equipo de cada sorteo, incluidos sus números de contacto.
L.2.1.4	Obligaciones del equipo del sorteo	*Control* Las instrucciones de funcionamiento incluirán las obligaciones de los miembros designados del equipo de cada sorteo.

L.2.1.5	Equipo de reserva para el sorteo	*Control* En las instrucciones de funcionamiento, se designarán a personas de reserva y se detallará su despliegue.
L.2.1.6	Horario del sorteo	*Control* Las instrucciones de funcionamiento incluirán horarios detallados del sorteo: desde la apertura hasta el cierre del lugar en que se llevará a cabo.
L.2.1.7	Observadores del sorteo	*Control* Las instrucciones de funcionamiento detallarán aquellas obligaciones previstas en la normativa de lotería sobre la presencia de observadores independientes durante un sorteo.

L.2.2 Realización del sorteo *Objetivo:* Garantizar que los sorteos transcurran conforme a los reglamentos aplicables y las normas del juego de lotería de que se trate.		
L.2.2.1	Procedimiento de sorteo	*Control* La organización definirá un procedimiento de sorteo exhaustivo para garantizar que todas sus funciones se lleven a cabo de acuerdo con las normas del juego de lotería de que se trate y los reglamentos aplicables.
L.2.2.2	Guía detallada del sorteo	*Control* El procedimiento de sorteo incluirá una guía detallada del proceso de sorteos.
L.2.2.3	Lugar del sorteo	*Control* El procedimiento de sorteo incluirá la definición del lugar del sorteo.
L.2.2.4	Asistencia al sorteo y responsabilidades	*Control* El procedimiento de sorteo incluirá una definición de la asistencia al sorteo, así como de las responsabilidades y actuaciones de todos los participantes.
L.2.2.5	Supervisión del sorteo	*Control* El procedimiento de sorteo definirá la política sobre la asistencia de un responsable de cumplimiento (independiente) o de un auditor.
L.2.2.6	Seguridad en el funcionamiento del sorteo	*Control* El procedimiento de sorteo incluirá medidas de seguridad adecuadas para el funcionamiento del sorteo y de todos los equipos que se utilicen durante el proceso de sorteo.
L.2.2.7	Emergencias durante el sorteo	*Control* El procedimiento de sorteo incluirá medidas que desplegar en caso de emergencia durante la realización del sorteo.
L.2.2.8	Alerta, comunicación e integridad del sorteo	*Control* La organización de lotería implementará un sistema o proceso para garantizar que ninguna persona o grupo con acceso al sistema central de juego manipule las transacciones antes, durante o después del sorteo y que se establezca una lista de verificación detallada del acceso del usuario, así como una auditoría de las transacciones.

L.2.3 Dispositivos físicos de sorteo y juegos de bolas *Objetivo:* Garantizar que los dispositivos físicos de sorteo y los juegos de bolas se ajusten a los requisitos de seguridad acordados y a las especificaciones reglamentarias.		
L.2.3.1	Procedimiento de inspección	*Control* Se definirá un procedimiento para inspeccionar los dispositivos de sorteo y los juegos de bolas, a su entrega y regularmente con posterioridad, entablando para ello las consultas pertinentes con una autoridad independiente (con el objeto el garantizar el cumplimiento de las especificaciones y las normas técnicas).
L.2.3.2	Inspección y mantenimiento regulares	*Control* Se realizarán y documentarán inspecciones y tareas de mantenimiento de los dispositivos de sorteo al menos una vez al año para que conserven durante toda su vida útil los estándares especificados.
L.2.3.3	Conjuntos de bolas compatibles	*Control* La organización definirá un procedimiento que prevea el uso de conjuntos de bolas fabricadas según los umbrales de medida y peso compatibles con la máquina de sorteo que vaya a utilizarse.
L.2.3.4	Dispositivos de sorteo de sustitución	*Control* La organización definirá un procedimiento que prevea la disponibilidad de un dispositivo de sorteo y conjuntos de bolas de sustitución que utilizar en caso de fallo mecánico o de otro tipo, cuando los sorteos se transmitan en directo.
L.2.3.5	Manipulación, almacenamiento y traslado de los dispositivos de sorteo y los conjuntos de bolas	*Control* La organización definirá un procedimiento para almacenar, trasladar y manipular de forma segura los dispositivos de sorteo y los conjuntos de bolas.
L.2.3.6	Transmisión del sorteo por medios tradicionales o vía Internet	*Control* Cuando los sorteos se transmitan en directo por medios tradicionales o vía Internet, se aplicará un procedimiento que minimice los riesgos asociados con la corrupción de datos, el retraso de audio o video, los errores en la generación de gráficos u otros que pudieran menoscabar la confianza del público en la integridad del sorteo.

L.3 Seguridad de los puntos de venta

L.3.1 Operaciones de los puntos de venta *Objetivo:* Garantizar que las operaciones de los puntos de venta, tanto a través como fuera de Internet, se ajusten a las obligaciones de seguridad que dicte la organización.		
L.3.1.1	Seguridad de los puntos de venta	*Control* La organización especificará en un contrato tanto las obligaciones como el entorno de seguridad en que el punto de venta deberá llevar a cabo su actividad.

L.3.2 Seguridad de los terminales de juego *Objetivo:* Garantizar una seguridad adecuada de los terminales de juego.		
L.3.2.1	Seguridad de las transacciones	*Control* Se protegerá el tráfico de datos entre los terminales de juego y el sistema central de juego y se aplicarán medidas para garantizar la integridad de las transacciones. En los casos que se utilice un dispositivo del punto de venta minorista en lugar de un terminal de juego exclusivo, se protegerá el tráfico de datos entre la aplicación de juego en el dispositivo del punto de venta y el sistema central de juego; no se fiará en la seguridad del dispositivo del punto de venta minorista para la integridad de los juegos.

L.4 Pago de premios

L.4.1 Validación y pago de premios *Objetivo:* Garantizar que la organización cuente con los controles necesarios para validar y abonar los premios, así como para prevenir el fraude con los premios sin reclamar.		
L.4.1.1	Proceso de validación	*Control* La organización definirá e implementará procedimientos para garantizar la validez de las transacciones, solicitudes y boletos ganadores para los diferentes niveles de premio y tipos de juego, y procesará los pagos de premios correspondientes.
L.4.1.2	Número de referencia único de los boletos	*Control* Cada boleto para cada juego dispondrá de un número de referencia único.
L.4.1.3	Seguridad de los datos de premios sin reclamar	*Control* La organización establecerá controles técnicos y de procedimientos a fin de garantizar la confidencialidad, integridad y disponibilidad de los datos de premios sin reclamar, incluidos, como mínimo, los archivos que contengan información de transacciones específicas que no se hayan reclamado y cualquier archivo de validación, entre otros. Se prestará una atención especial al control de acceso para restringir el acceso a los datos y controlar la interacción del usuario con estos; se creará un procedimiento para tratar los casos de acceso no autorizado y de exportación de datos.
L.4.1.4	Procedimiento para el pago de premios	*Control* Se establecerá un procedimiento para el pago de premios que: establezca un plazo máximo para el reclamo de premios, incluya un proceso para auditar las transferencias definitivas una vez liquidado el juego, especifique las normas y la debida diligencia necesaria antes de tomar decisiones respecto del pago de boletos perdidos, robados o dañados y explique el procedimiento relativo a las consultas sobre la validez de las solicitudes. Asimismo, se definirá un procedimiento sobre los retrasos en los pagos o los pagos de última hora.
L.4.1.5	Detección de fraudes	*Control* Se mantendrán registros de auditoría adecuados y se revisarán como parte del procedimiento de pago de premios para identificar patrones inusuales de pagos con retraso y reclamos de los puntos de venta que pudieran requerir investigación.

L.4.1.6	Supervisión del porcentaje de pagos de premios	*Control* Se controlarán la seguridad y el porcentaje de pago de premios de los juegos.
L.4.1.7	Procedimiento para resolver disputas o reclamaciones	*Control* Se documentarán procedimientos para gestionar disputas o reclamaciones de clientes con respecto a ganancias o pérdidas.

L.5 Métodos de pagos y cuentas de jugador

L.5.1 Seguridad de los métodos de pago

Objetivo: Proteger los métodos de pago de usos fraudulentos.

L.5.1.1	Compilación de datos	*Control* La compilación de datos sensibles relacionados directamente con los pagos se limitará a datos estrictamente necesarios para la transacción.
L.5.1.2	Protección del método de pago	*Control* Se adoptarán medidas adecuadas para proteger de usos fraudulentos cualquier tipo de pago que se utilice en el sistema.
L.5.1.3	Autorización del servicio de pago	*Control* La organización verificará que el servicio de pago garantice la protección de los datos del jugador, incluida toda información personalmente identificable que facilite el jugador, y de los datos sobre los pagos.

L.5.2 Cuenta de jugador

Objetivo: Proteger al jugador y gestionar el riesgo de fraude y blanqueo de capitales en los sistemas de juego que requieran identificación de los jugadores.

L.5.2.1	Cuenta de jugador	*Control* Existirá un proceso formal para identificar, autenticar y autorizar a los jugadores. Tanto los datos del jugador como la billetera se considerarán activos críticos a efectos de evaluación de riesgos.
L.5.2.2	Diversas cuentas de jugador	*Control* Se tomarán medidas razonables para garantizar que cada jugador posea solo una cuenta activa.
L.5.2.3	Exclusión de jugadores	*Control* Se definirá un proceso para excluir jugadores de acuerdo con las leyes locales aplicables o los procedimientos internos.
L.5.2.4	Titular de múltiples instrumentos de pago	*Control* Se definirá un procedimiento, conforme a las leyes locales aplicables, para garantizar que el titular del instrumento de pago sea efectivamente el titular de la cuenta de jugador a fin de evitar el fraude y el lavado de dinero.

L.5.2.5	Registros de transacciones relacionados con pagos	*Control* La organización generará todos los registros de transacciones de las cuentas de jugador. Los datos registrados permitirán a la organización identificar individualmente cada actividad financiera de cada jugador.

L.6 Apuestas deportivas, de deportes electrónicos y de carreras de caballos

L.6.1 Selección de la oferta

Objetivo: Garantizar la integridad de la oferta de apuestas.

L.6.1.1	Marco de las apuestas	*Control* Se definirá, mantendrá y publicará el marco en que la organización ofrece apuestas deportivas, de deportes electrónicos y de carreras de caballos, así como las reglas, entre otros, correspondientes a todos los tipos de eventos deportivos autorizados y todos los tipos de apuestas autorizadas para cada deporte que se oferte.

L.6.2 Gestión de eventos, probabilidades y resultados

Objetivo: Garantizar la integridad de los eventos y sus correspondientes probabilidades.

L.6.2.1	Gestión de eventos, probabilidades y resultados	*Control* Se definirán procedimientos para seleccionar los eventos, configurar y actualizar las probabilidades, los márgenes de apuestas o el bloqueo de eventos, así como para recibir los resultados de fuentes confiables. Se dispondrá de un proceso para validar la precisión y prevenir actividades fraudulentas. Los procedimientos se basarán en el respeto de la integridad, el juego responsable y la garantía de la transparencia.
L.6.2.2	Apuestas en directo	*Control* Se documentarán procedimientos para garantizar y seguir la integridad de la oferta de apuestas en directo, la gestión de los resultados y la protección de los clientes. Los ámbitos indicativos que deberán considerarse en el procedimiento para la gestión de resultados incluyen, entre otros, la demora, las fuentes de resultados y la reversión de resultados. Asimismo, los procedimientos contemplarán mecanismos de prevención de la provisión de información desde el lugar del evento que incluya, entre otras cosas, la demora en la transmisión de resultados durante eventos en directo.
L.6.2.3	Protección de los niveles de pago	*Control* La organización definirá un conjunto de medidas para garantizar que no se superen los niveles autorizados de pago.

L.6.3 Control para combatir el fraude y el blanqueo de capitales

Objetivo: Garantizar actuaciones para minimizar el riesgo de fraude o blanqueo de capitales.

L.6.3.1	Seguimiento de las actividades de apuestas deportivas	*Control* Se definirán procedimientos para realizar el seguimiento de todos los cambios en las probabilidades o los bloqueos durante un evento deportivo, de deporte electrónico o carrera de caballos, del mercado, de los eventos y de las transacciones de los clientes para detectar irregularidades y hacer seguimiento de los ganadores que superen un determinado importe de ganancias y de los ingresos que excedan un monto determinado. Asimismo, los procedimientos especificarán los umbrales de pago y los métodos de cobro. Los procedimientos deberán establecerse de conformidad con las leyes de la jurisdicción en la que se encuentra domiciliado el miembro que se certifica.

L.7 Terminales de videolotería interactivos

Terminales de videolotería (VLT)

Objetivo: Garantizar la seguridad en el funcionamiento de los VLT con independencia del diseño del sistema o el modelo operativo.

L.7.1.1	VLT	*Control* Se controlarán la seguridad y el porcentaje de pago de premios de los VLT.
L.7.1.2	Juegos mediante VLT	*Control* Se pondrán a disposición del cliente las reglas de los juegos y el porcentaje total de pago de premios.
L.7.1.3	Certificación de los juegos para VLT	*Control* Los juegos específicos para VLT se verán sometidos a las pruebas correspondientes y se mantendrá/emitirá una certificación de integridad y pago de premios.
L.7.1.4	Arquitectura de los sistemas de VLT	*Control* La organización dispondrá de una descripción de la arquitectura global de los sistemas de VLT, incluidas las medidas de seguridad, para garantizar la integridad de los juegos de VLT y la seguridad en el tratamiento y almacenamiento de los datos.

L.8 Generación de números aleatorios

L.8.1 Aleatoriedad de los sorteos electrónicos y de los juegos de azar digitales

Objetivo: Garantizar la integridad y equidad de los generadores de números aleatorios y de los algoritmos de sorteos mediante protección física y lógica. El control L.8 abarca los sorteos electrónicos y los juegos de azar digitales.

L.8.1.1	Protección física y lógica del sistema técnico	*Control* Se adoptarán medidas para garantizar que solo las personas autorizadas puedan acceder físicamente al generador de números aleatorios (fuente de entropía) y al algoritmo de sorteo, así como que se les brinde protección lógica, a fin de evitar cualquier modificación en la configuración del algoritmo y de la fuente de entropía. Los sistemas físicos se protegerán de robos, modificaciones no autorizadas e interferencias.

L.8.1.2	Seguridad en las transmisiones	*Control* Se adoptarán medidas para garantizar la integridad y la autenticidad de los datos que se transmitan entre el generador de números aleatorios (fuente de entropía) y el algoritmo de sorteo.
L.8.1.3	Verificación de la aleatoriedad e integridad de los sorteos electrónicos	*Control* Antes de su despliegue, se realizarán pruebas y verificaciones a cargo de partes independientes con el fin de verificar la aleatoriedad del sistema de sorteo electrónico. La organización documentará su política sobre pruebas y verificaciones posteriores al despliegue para comprobar que el generador de números aleatorios y el algoritmo de sorteo funcionan como previsto.
L.8.1.4	Separación de responsabilidades	*Control* Además del control G.2.1.7, se adoptará un procedimiento específico con respecto a la separación de las responsabilidades involucradas en un sorteo electrónico para evitar fraude interno. Concretamente, ninguna persona podrá desempeñar más de uno de los siguientes tipos de responsabilidades: mantenimiento, seguimiento o realización de sorteos mediante equipos electrónicos de juego.

L.9 Juegos en línea

L.9.1 Juegos en línea

Objetivo: Garantizar el funcionamiento seguro de los juegos
Se refiere a toda actividad relacionada con el juego que se ofrece a través de una aplicación móvil o de plataformas web, excluidas las transacciones minoristas.

L.9.1.1	Reglas del juego en línea	*Control* Se pondrán a disposición del cliente las reglas del juego en línea y el porcentaje total de pago de premios.
L.9.1.2	Certificación de los juegos en línea	*Control* Los juegos en línea se verán sometidos a las pruebas correspondientes y se proporcionará evidencia de la integridad y del correcto pago de premios durante el ciclo de vida del juego.
L.9.1.3	Salida de los juegos en línea	*Control* Se establecerán procedimientos aplicables cuando los juegos en línea salgan de producción, que incluya, por ejemplo, cómo manejar los premios que no se han ganado.
L.9.1.4	Discrepancias de los resultados de juegos en línea	*Control* Se establecerán procedimientos para el manejo de discrepancias entre lo que se presenta en los dispositivos digitales del cliente y lo que está registrado en el sistema de juego.
L.9.1.5	Seguridad de los juegos con ganadores predeterminados	*Control* Para los juegos con ganadores predeterminados, se establecerán procedimientos basados en un análisis de riesgos para garantizar que nadie pueda aprovecharse de los mecanismos del juego.

L.10 Diseño de juegos y aprobación

L.10.1 Diseño de juegos y aprobación

Objetivo: Garantizar que los diseños de los juegos cumplan los requisitos legales y normativos y cuenten con la correspondiente autorización antes de su activación.

L.10.1.1	Documentación de los procedimientos de juego	*Control* Se documentarán las reglas del juego y serán de fácil acceso para los jugadores.
L.10.1.2	Aprobación y modificación de los juegos	*Control* Se definirá un procedimiento de aprobación para validar el control de cada juego nuevo y de las modificaciones relevantes que se produzcan en los sistemas digitales de juego. Los diseños definitivos de los juegos se autorizarán formalmente mediante un proceso en el que participe la función de seguridad.
L.10.1.3	Selección de un proveedor de juegos	*Control* La función de seguridad deberá participar en el proceso de aprobación.

Anexo C (controles «S»): controles para el desarrollo de sistemas de juego y la prestación de servicios de juego

Los controles S se aplican al desarrollo de sistemas de juego y a la prestación de servicios de juego, bien sea por parte de un proveedor de juegos o de los desarrolladores internos del operador de juegos. En el caso en el que un operador de juegos o un proveedor de juegos adquiera un sistema o servicios de juegos de un tercero, deberá asegurarse de que el tercero respete los controles S.

S.1 Garantía de seguridad de los sistemas de juego		
S.1.1 Desarrollo seguro de las aplicaciones de sistemas de juego *Objetivo:* Garantizar la seguridad en el diseño de los sistemas de juego.		
S.1.1.1	Política de seguridad para el desarrollo de aplicaciones	*Control* Se dispondrá de una política en materia de seguridad en las aplicaciones durante todo el período de su desarrollo.
S.1.1.2	Pruebas de seguridad	*Control* La organización realizará pruebas de seguridad de sus productos y servicios, y adaptará las pruebas en función de la naturaleza del cambio, considerando el impacto y el nivel de riesgo asociado. Asimismo, la organización facilitará al proveedor: • un inventario de las pruebas realizadas durante el desarrollo de la aplicación. Dicho inventario abarcará los riesgos principales. • un resumen de los resultados junto con las notas de lanzamiento de su producto a un entorno de producción tanto del lanzamiento inicial como de cualquier relanzamiento subsiguiente significativo.
S.1.1.3	Representatividad de las pruebas de seguridad	*Control* Las pruebas de seguridad realizadas por el proveedor de tecnología de juegos mostrarán cómo el operador desplegará el sistema en un entorno de producción.
S.1.1.4	Prácticas de codificación segura	*Control* Se establecerá un conjunto de prácticas de codificación segura que los desarrolladores deberán seguir. Asimismo, se aplicarán medidas para verificar la efectividad y el cumplimiento de dichas prácticas.
S.1.1.5	Capacitación y concienciación en codificación segura	*Control* Se dispondrá de un programa de capacitación y concienciación en prácticas de codificación segura para todos los desarrolladores de códigos para los sistemas de juego.

S.1.2 Medidas de integridad relativas al desarrollo de equipos, programas y controladores de los sistemas de juego *Objetivo:* Garantizar la integridad de las tecnologías de juego.		
S.1.2.1	Controles de integridad durante el proceso de desarrollo	*Control* Habrá garantía de la integridad de los programas y controladores que se desarrollen en cada etapa del proceso de desarrollo, incluido al menos, durante el proceso de control de calidad y de despliegue de los programas y controladores en el entorno de producción, entre otros.
S.1.2.2	Registro de seguridad	*Control* Se contará con los registros de seguridad adecuados de los programas / controladores desarrollados, que el equipo de seguridad pueda integrar a las herramientas de seguridad a fin de garantizar la integridad de los programas y controladores. Se creará un documento que explique cómo interpretar el registro de seguridad.
S.1.2.3	Integridad de los archivos	*Control* Se identificarán y documentarán los archivos críticos en el producto a fin de que el operador de juegos verifique la integridad del entorno de producción.
S.1.2.4	Integridad de los equipos	*Control* Se adoptarán medidas para identificar intentos no autorizados de agregar o modificar los equipos de los sistemas de juego que pudieran afectar la integridad del sistema de juego. En este contexto, los equipos incluyen como mínimo, los terminales de videolotería, los equipos del punto de venta de juegos, así como los generadores de números aleatorios, entre otros. La lista completa de los equipos a los que se aplica este control se determinará mediante una evaluación de riesgos. Estarán exentos de este control los equipos suministrados y hospedados por un proveedor de infraestructura como servicio.
S.1.2.5	Gestión de parches y vulnerabilidades	*Control* Se dispondrá de un proceso para actualizar de manera oportuna los programas/ controladores y cualquier biblioteca de códigos externa que se utilice. Una evaluación de riesgos permitirá decidir si se aplican o no parches al sistema de producción de juegos, tomando en cuenta la política de gestión de parches y vulnerabilidades del operador de juegos, así como las consideraciones comerciales.
S.1.2.6	Divulgación responsable	*Control* El proveedor de juegos pondrá a disposición de todos aquellos que adquieran sus productos o servicios una política de divulgación responsable para la divulgación de las vulnerabilidades de seguridad en sus productos de sistemas de juego.

S.1.3 Medidas de integridad relativas a la impresión de boletos físicos para juegos instantáneos *Objetivo:* Garantizar la integridad de los boletos físicos para juegos instantáneos.		

S.1.3.1 Obligaciones para juegos instantáneos en físico *Objetivo:* Alinear las especificaciones del proveedor con las obligaciones del juego.		
S.1.3.1.1	Obligaciones para juegos instantáneos	*Control* El fabricante validará formalmente las obligaciones con el operador de juegos y los traducirá en especificaciones; cualquier cambio en las especificaciones seguirá el proceso de gestión de cambios tanto del operador de juegos como del proveedor.

S.1.3.2 Creación y validación de los datos *Objetivo:* Garantizar la seguridad y la conformidad con los requisitos de la programación de los juegos instantáneos.		
S.1.3.2.1	Generación de datos de los juegos instantáneos	*Control* El proceso de aleatorización empleado para la generación de los datos de juegos instantáneos está sujeto a la aplicación de los controles contemplados en la sección L.8 de este Estándar «Generación de números aleatorios» y a los requerimientos acordados entre el operador y el proveedor.
S.1.3.2.2	Validación de los datos de juego	*Control* El fabricante del boleto garantizará que un equipo independiente valide los datos lógicos del juego con los requisitos del operador de juegos. Los resultados se pondrán a disposición del operador de juegos.
S.1.3.2.3	Confidencialidad de los datos	*Control* El fabricante del boleto garantizará que el acceso a los datos de validación permanezca restringido en todo momento, incluso luego de la ejecución del juego instantáneo, de conformidad con el principio del mínimo privilegio.

S.1.3.3 Impresión *Objetivo:* Garantizar la integridad en el proceso de impresión.		
S.1.3.3.1	Validación previa a la impresión	*Control* El fabricante del boleto validará formalmente con el operador de juegos los textos e imágenes finales de los boletos antes de su impresión.
S.1.3.3.2	Pruebas de integridad	*Control* El fabricante del boleto realizará con regularidad auditorías de integridad de los boletos.

S.1.3.4 Detalles finales *Objetivo:* Garantizar la conformidad con la estructura de premios y la integridad de los boletos durante el envío.		
S.1.3.4.1	Número de referencia único de los boletos	*Control* Se tomarán las medidas necesarias para que cada boleto entregado tenga un número de referencia único.
S.1.3.4.2	Conformidad con la estructura de premios	*Control* El proveedor proporcionará evidencias de que ha impreso el número exacto de boletos en cada lote conforme a la estructura de premios requerida.
S.1.3.4.3	Boletos anulados	*Control* Se documentará un procedimiento para garantizar la destrucción segura de los boletos impresos que no se hayan entregado.
S.1.3.4.4	Seguridad en el envío	*Control* El proveedor garantizará la seguridad en la entrega de los boletos al operador de juegos.

Anexo D (controles «M»): Controles para juegos multijurisdiccionales

M.1 Obligaciones para participar en juegos administrados por la Asociación Multiestatal de Loterías de los Estados Unidos (MUSL, por sus siglas en inglés)		
M.1.1 Seguridad, integridad y disponibilidad de las transacciones *Objetivo:* Garantizar el registro adecuado y la seguridad de las transacciones.		
M.1.1.1	Validación de solicitudes	*Control* Además de cumplir con las obligaciones de los controles contemplados en la sección L.4.1 de este documento, las organizaciones mostrarán conformidad con los estándares mínimos de seguridad del juego de la MUSL.
M.1.1.2	Redundancia de los datos de transacciones	*Control* Se guardarán registros de los datos de transacciones vendidas en el sistema de juego informatizado en al menos dos ubicaciones distintas del centro de datos y estarán suficientemente separados de manera que no estén sujetos al mismo desastre.
M.1.1.3	Confirmación de recepción de las transacciones	*Control* Cada ubicación recibirá y confirmará la recepción de los datos de transacciones antes de que se autorice la impresión de los boletos.
M.1.1.4	Copia de seguridad de los datos del juego	*Control* Diariamente se creará una copia de seguridad de los datos del juego y se almacenarán fuera de línea y en otras instalaciones.
M.1.1.5	Integridad de las transacciones antes y después de cada sorteo	*Control* Se aplicará una función hash criptográfica aprobada por la MUSL a todo el conjunto de transacciones almacenadas a través del sistema de control interno antes de cada sorteo con la finalidad de crear una síntesis del mensaje. Se aplicará nuevamente la misma función hash criptográfica a todo el conjunto de transacciones luego de la creación de un informe de ganadores por nivel inmediatamente después del sorteo.

M.1.2 Seguridad del dispositivo del punto de venta minorista *Objetivo:* Garantizar la seguridad de los dispositivos del punto de venta minorista que no sean terminales exclusivos de lotería.		
M.1.2.1	Dispositivo del punto de venta minorista	*Control* En los casos que se utilice un dispositivo del punto de venta minorista en lugar de un terminal exclusivo de lotería, el dispositivo del punto de venta minorista debe conformarse a las obligaciones de la Asociación Norteamericana de Loterías Estatales y Provinciales (NASPL).

M.1.2.2	Terminales de lotería no diseñados para emitir boletos *in situ*	*Control* Se modificarán los terminales de lotería que no estén diseñados para emitir boletos *in situ*, y a los cuales tengan acceso los operadores del sistema informatizado de juego o del sistema de control interno, de manera que quede claro que cualquier boleto emitido por dichos terminales no es válido. Ni las operaciones que se realicen en el sitio ni el personal de TI podrá evitar que se realicen tales modificaciones.

M.1.3 Apuesta rápida aleatoria (Quick picks) *Objetivo:* Garantizar la aleatoriedad del sistema de apuesta rápida.		
M.1.3.1	Aleatoriedad de la apuesta rápida	*Control* Los programas empleados para generar números aleatorios para la apuesta rápida cumplirán con el control L.8.1.3 de este estándar «Verificación de la aleatoriedad e integridad de los sorteos electrónicos».

M.1.4 Separación entre el sistema de control interno y el sistema informatizado de juego *Objetivo:* Garantizar la separación entre el sistema de control interno y el sistema informatizado de juego (ICS y CGS respectivamente, por sus siglas en inglés).		
M.1.4.1	Separación entre el sistema de control interno y el sistema informatizado de juego	*Control* Con respecto al control L.2.2.8 de este estándar « Alerta, comunicación e integridad del sorteo », si un proveedor externo opera el sistema informatizado de juego, una organización diferente operará el sistema de control interno. En cualquier caso, se separará la responsabilidad de cada uno de estos sistemas y ninguna persona tendrá acceso total o parcial a ambos sistemas: el ICS y el CGS.

M.1.5 Procedimiento del sorteo *Objetivo:* Garantizar la continuidad e integridad entre el tratamiento de los números ganadores y el tratamiento de las transacciones de venta.		
M.1.5.1	Uso del mismo personal y del mismo sistema de control interno	*Control* La organización de lotería, o la organización por ella designada y autorizada, procesará los números ganadores empleando el mismo personal y los mismos sistemas ICS que usan para el tratamiento de las transacciones de venta.

M.1.6 Sistema de detección de intrusos *Objetivo:* Gestionar el riesgo de ciberataques a los sistemas ICS y CGS.		
M.1.6.1	Sistema de detección de intrusos en las redes de los sistemas ICS y CGS	*Control* Se establecerá un sistema de detección de intrusos y comunicación o un sistema de prevención de intrusos en las redes de los sistemas ICS y CGS y se configu-rarán de manera que notifiquen a los administradores locales.