Asociación Mundial de Loterías

WLA-SCS:2020

WLA – Estándar de control de seguridad

Obligaciones de seguridad e integridad de la información y las operaciones para organizaciones de lotería, apuestas deportivas y sus proveedores.

Publicación: octubre de 2020, Versión 1.1
(Revisada: 10 de diciembre de 2020)

Índice

Preámbulo

La Asociación Mundial de Loterías (WLA, por sus siglas en inglés) reconoce desde su fundación la necesidad de que las organizaciones de loterías y apuestas deportivas dispongan de un estándar de seguridad e integridad adecuado, motivo por el cual ha seguido adelante con el trabajo iniciado por sus predecesores.

Las organizaciones de lotería y apuestas deportivas tienen la obligación comercial de desarrollar entornos que hagan posible mantener una postura visible y documentada de seguridad e integridad con el fin de conservar la confianza de los jugadores y de otras partes interesadas. El estándar de control de seguridad de la WLA (SCS de la WLA, por sus siglas en inglés) tiene por objeto ayudar a las organizaciones de lotería y apuestas deportivas 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 del sector, reforzándose de esta manera la confianza en la integridad de las operaciones de las organizaciones de lotería y apuestas deportivas. La certificación en el SCS de la WLA ofrece una medida objetiva del rendimiento de dichas organizaciones en cuanto al control de la seguridad y la gestión de riesgos.

El desarrollo del SCS de la WLA corre a cargo del Comité de Seguridad y Gestión de Riesgos de la WLA (SRMC de la WLA). Pertenecen al SRMC de la WLA representantes y especialistas en seguridad de organizaciones de lotería y apuestas deportivas de todo el mundo. Comparar las prácticas actuales de seguridad e integridad en el sector con las aprobadas por expertos en lotería de todo el mundo ha permitido definir un marco sólido de seguridad y gestión de riesgos para las organizaciones de lotería y apuestas deportivas.

El SRMC de la WLA evalúa todos los estándares de control de seguridad para su uso por el sector de la lotería y las apuestas deportivas, actúa como referencia para el sector en lo referente a cuestiones de seguridad y supervisa el proceso de certificación, mediante el cual se verifica el cumplimiento con el SCS de la WLA de los miembros y miembros asociados de la WLA.

Todos los estándares emanados del SRMC de la WLA, con independencia de que sean de nuevo cuño o que respondan a actualizaciones, 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 mantener su SCS actualizado y adaptado para observar la norma ISO/IEC 27001.

Introducción

El presente estándar define el nivel de seguridad, integridad y gestión de riesgos que debe aplicar el sector de la lotería y las apuestas deportivas; su objetivo es actuar 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 comunes de seguridad que representan buenas prácticas para las organizaciones de lotería y apuestas deportivas. El estándar incluye un conjunto integral de controles y obligaciones para las organizaciones de lotería y apuestas deportivas, así como para sus proveedores.

Asimismo, puede considerarse la base para fraguar relaciones de confianza con reguladores y partes interesadas del sector a fin de desempeñar operaciones de lotería y apuestas deportivas o juegos multijurisdiccionales, y puede contribuir sustancialmente a su gestión eficaz, al ofrecer una valoración independiente con el fin de fomentar una mayor confianza en la seguridad de las operaciones de lotería y apuestas deportivas.

La más reciente versión del estándar, WLA-SCS:2020, presenta un nuevo marco de certificación en dos niveles.

El cumplimiento con el Nivel 1 del SCS de la WLA confirma que el operador de lotería y apuestas deportivas 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 SCS de la WLA, el Nivel 2. La certificación en el Nivel 1 del SCS de la WLA es ideal para las organizaciones miembro de la WLA que prefieren un enfoque gradual para la certificación.

Por su parte, el cumplimiento con el Nivel 2 del SCS de la WLA 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 específicos para organizaciones de lotería y apuestas deportivas y el cumplimiento con la norma ISO/IEC 27001 para los Sistemas de Gestión de la Seguridad de la Información, el Nivel 2 del SCS de la WLA representa el estándar de certificación más completo y extenso disponible tanto para organizaciones de lotería y apuestas deportivas como para sus proveedores.

La adopción del SCS de la WLA supone una decisión estratégica. Inciden en la concepción y la aplicación de los sistemas de gestión de la seguridad y la integridad de una organización sus necesidades, sus objetivos, sus riesgos y sus requisitos de seguridad específicos, los procesos empleados, así como las dimensiones y la estructura de la organización. Se prevé que estos factores y sus sistemas de respaldo cambien con el tiempo; 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 precisa de un sistema sencillo –.

El cumplimiento del SCS de la WLA podrán utilizarlo las partes interesadas internas y externas para evaluar la seguridad y la integridad de los sistemas tanto de las organizaciones de lotería y apuestas deportivas, como de sus proveedores.

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

1. Ámbito del estándar

El SCS de la WLA abarca todo tipo de organizaciones de lotería y apuestas deportivas, incluidas empresas comerciales, organismos públicos y organizaciones sin ánimo de lucro.

El SCS de la WLA 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 SCS de la WLA son genéricos y tienen como fin resultar aplicables a todas las organizaciones, con independencia de su tipología, sus dimensiones y su naturaleza. En cualquier caso, si una organización desea declarar su conformidad con el SCS de la WLA, esta no podrá excluir ninguno de los controles previstos en los Anexos A, B, C o D.

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 SCS de la WLA, 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 ámbito de certificación descrito en el certificado del SCS de la WLA, 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 SCS de la WLA en el seno del sistema de gestión existente.

Importante: El SCS de la WLA no pretende incluir todas las estipulaciones necesarias de un contrato. Los miembros de la WLA que adopten el SCS de la WLA 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 Tecnologías de la información – Técnicas de seguridad – Sistemas de gestión de la seguridad de la información – Obligaciones.

ISO/IEC 27017 Tecnologías de la información – Técnicas de seguridad – Código de prácticas para los controles de seguridad de la información en base a la norma ISO/IEC 27002 para los servicios en la nube.

WLA-SCS:2020 Código de prácticas – directrices de mejores prácticas para los controles y las obligaciones de seguridad e integridad del SCS de la WLA.

Guía de certificación en el SCS de la WLA.

3. Términos y definiciones

3.1 Abreviaturas

WLA: Asociación Mundial de Loterías

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

SRMC de la WLA: Comité de Seguridad y Gestión de Riesgos de la WLA

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: Se trata de cualquier empleado, contratista u otro tercero que trabaja para la organización de lotería o el proveedor de tecnología de lotería y que, por su función o acceso, tiene el potencial de afectar la confidencialidad, disponibilidad o integridad de la lotería.

Sistema de juego: Se refiere a los sistemas que se requieren para operar juegos, incluidos tanto el sistema central de juego como cualquiera de sus componentes periféricos necesarios para operar dichos juegos.

Sistemas de juego digitales: Toda la tecnología que permite ofrecer juegos a través de un canal de venta digital.

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 el funcionamiento de una organización de lotería y apuestas deportivas es clave para conservar a los jugadores y demás partes interesadas. Por tanto, las organizaciones miembro de la WLA deben desarrollar y mantener un entorno de seguridad e integridad visible y documentado.

El SRMC de la WLA describe en el SCS las obligaciones, los objetivos y los controles de supervisión que se consideran prácticas óptimas. Las organizaciones de lotería y apuestas deportivas dispondrán de un sistema de gestión de la 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 SCS de la WLA incorpora obligaciones y controles de referencia en los procesos generales de seguridad, integridad y gestión de riesgos de las organizaciones de lotería y apuestas deportivas, evitando interferencias con marcos de seguridad más generales. Ofrece a los profesionales de seguridad e integridad del sector de la lotería y las apuestas deportivas

un proceso con el que gestionar formalmente, actualizar y mejorar sus controles de forma continua. Por tanto, las organizaciones de lotería y apuestas deportivas deben desarrollar y mantener un entorno de seguridad visible y documentado.

El SCS de la WLA comprende cuatro partes en las que se especifican los controles mínimos necesarios para la gestión eficaz de la seguridad y la integridad de una organización de lotería y apuestas deportivas, así como de los proveedores a la industria.

La primera parte (Anexo A – Controles «G»: controles para todas las organizaciones) incluye el cumplimiento con la norma ISO/IEC 27001 dentro de un enfoque global, además de 24 controles básicos adicionales de la WLA.

La segunda parte (Anexo B – Controles «L»: controles para operadores de lotería) proporciona 64 controles adicionales de seguridad e integridad específicos para operadores de loterías y apuestas deportivas, que representan las mejores prácticas actuales.

La tercera parte (Anexo C – Controles «S»: controles para operadores y proveedores de sistemas de juego) contiene 21 controles basados en productos y servicios que ofrecen los proveedores de loterías y apuestas deportivas.

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 Estados Unidos (MUSL, por sus siglas en inglés).

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

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

Las organizaciones que deseen certificarse en el Nivel 2 del WLA-SCS:2020 deben contar con un sistema de gestión de la seguridad de la información (ISMS, por sus siglas en inglés) que se ajuste a los requisitos previstos en la norma ISO/IEC 27001.

5.2 Ámbito del ISMS

El ISMS de la organización abarcará todas las actividades de lotería y apuestas deportivas que explote, incluidos todos los activos y los sistemas de información conexos. Su ámbito únicamente podrá excluir aquellas operaciones de la organización ajenas a actividades de lotería y apuestas deportivas. 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 la concepción de las operaciones de lotería y apuestas deportivas se encuentran incluidas en el ámbito del ISMS.

5.3 Declaración de aplicabilidad

La declaración de aplicabilidad del ISMS de la organización debe incluir expresamente todos los controles que se prevén en los Anexos A, B, C y D del SCS de la WLA. No podrá excluirse ningún control, aunque algunos de los que contempla el Anexo B y C pueden resultar no aplicables. Las declaraciones de ausencia de aplicabilidad deberán justificarse de manera exhaustiva.

Una vez declarada su conformidad con el SCS de la WLA, una organización no podrá excluir las obligaciones que se especifican en esta cláusula ni ninguno de los controles previstos en los Anexos A, B, C y D.

Cualquier ausencia de aplicabilidad de los controles incluidos en el Anexo B y C que resulte necesaria deberá justificarse formalmente y deberán aportarse evidencias de que dicha ausencia de aplicabilidad cuenta con la aceptación del personal responsable de la organización. En los casos en que algún control resulte no aplicable, no se aceptarán declaraciones de conformidad, salvo que tales exclusiones no afecten 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.

Anexo A (controles «G»): controles para todas las organizaciones

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 ISMS 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, incluyendo, entre otros, 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	Atenciones de hostelería u obsequios	*Control* El código de conducta incluirá disposiciones contra la corrupción, que abarcarán las atenciones de hostelería y los obsequios que se reciban de personas o entidades con las que la organización mantenga una relación comercial o que se les ofrezcan.
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 de la organización de lotería).
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 lotería de proteger la integridad de los juegos.
G.2.1.7	Separación de funciones	*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. En el caso de los proveedores de tecnología de lotería, se aplicará este control a las áreas críticas de codificación que pudieran afectar la integridad de un juego como la gestión de la información del generador de números aleatorios empleado para determinar el resultado de los juegos, entre otros.

G.2.2	Protección del personal	
Objetivo:	Garantizar un nivel adecuado de protección para el personal.	
G.2.2.1	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 de lotería 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 juego.	
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.

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. Los proveedores de tecnología 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 junto con el responsable del proceso, la función de TI y la función de seguridad.
G.4.1.2	Registro del 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	Mantenimiento de sistemas de información	
G.5.1	**Controles criptográficos**	
Objetivo:	Proteger la confidencialidad, la autenticidad y la integridad de las claves criptográficas y de los datos importantes sobre juego, lotería y clientes por medios criptográficos.	
G.5.1.1	Controles criptográficos para la confidencialidad y la integridad de datos en reposo en sistemas portátiles y terminales de lotería	*Control* Se cifrará la información sensible almacenada en sistemas informáticos portátiles (en dispositivos de usuario final, por ejemplo, ordenadores portátiles o en medios informáticos removibles, como dispositivos USB y otros similares) para proteger la confidencialidad de la información y la integridad de la información sensible en reposo en terminales de lotería.
G.5.1.2	Controles criptográficos para la confidencialidad y la integridad de los datos en tránsito por redes	*Control* Para proteger la confidencialidad y la 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 u otros de relevancia sobre juegos, clientes y 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 y datos 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 servicios en la nube	
Objetivo:	Garantizar la seguridad de la información de los sistemas de lotería hospedados en la nube.	
G.5.3.1	Seguridad de servicios en la nube	*Control* Los entornos de nube que hospedan sistemas de juego deberán cumplir con la norma ISO/IEC 27017. Se define como un entorno de nube a una plataforma externa manejada por un tercero que ofrece una serie de aplicaciones a la que la organización se suscribe para recibir servicios como: infraestructura como servicio, plataforma como servicio, software como servicio, entre otros, necesarios para su funcionamiento. Los proveedores de tecnología deberán aplicar los controles descritos en la sección G.5.3 del SCS de la WLA a los repositorios de códigos empleados para desarrollar sistemas de juego.

G.6 Disponibilidad del sistema y continuidad empresarial

G.6.1	Disponibilidad de los servicios y continuidad empresarial	
Objetivo:	Garantizar la protección de la imagen y la reputación de la organización y contrarrestar 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 de lotería, así como las obligaciones de disponibilidad y resiliencia de dichos servicios. Los sistemas se diseñarán conforme a esas obligaciones.
G.6.1.2	Continuidad empresarial	*Control* La organización preparará un plan de continuidad empresarial documentado que abarque, como mínimo, el funcionamiento continuo de los juegos de lotería y la confianza continua de las partes interesadas en la integridad de las operaciones de lotería. 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 empresarial.

Anexo B (controles «L»): controles para operadores de lotería

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 las obligaciones legislativas y reglamentarias; garantizar la integridad del juego y prevenir el fraude.	
L.1.1.1	Selección del proveedor/ imprenta	*Control* Se establecerá un proceso formal de aprobación en el que participe la función de seguridad.
L.1.1.2	Obligaciones y pruebas de integridad	*Control* La organización documentará un procedimiento en el que especifique las obligaciones de integridad para cada juego instantáneo durante todo el ciclo de vida del juego, desde su diseño hasta su destrucción. Las obligaciones de integridad incluirán, como mínimo, lo siguiente: texto e imágenes finales, estructura de premios, protección de los archivos de validación/ganadores, controles de calidad, existencias auditables para distribución, ubicación de los paquetes y pruebas adecuadas de los requisitos antes de la aceptación del juego.
L.1.1.3	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.1.1.4	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 del lugar en que se llevará a cabo hasta su cierre.
L.2.1.7	Observadores del sorteo	*Control* Las instrucciones de funcionamiento detallarán aquellas obligaciones previstas en la normativa de lotería sobre 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 los 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 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 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 de 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 retransmitan 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 gestionar 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 retransmitan 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.2.4	**Sorteos de lotería y juegos instantáneos electrónicos**	
Objetivo:	Garantizar la integridad del sistema electrónico de sorteo con medidas de protección físicas y lógicas. Esta sección cubre tanto los juegos por sorteo como los juegos con premios instantáneos por medios electrónicos.	
L.2.4.1	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.2.4.2	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.2.4.3	Verificación de la aleatoriedad y la 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 se ajustan a las especificaciones.
L.2.4.4	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.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* Para garantizar que los puntos de venta cumplan las obligaciones de seguridad de la organización, esta 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 exclusivo de lotería, se protegerá el tráfico de datos entre la aplicación de lotería 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 de lotería.

L.4	Pago de los 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 diferentes niveles de premio y tipos de juego, así como un proceso para el pago de premios.
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, la integridad y la 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 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 del personal o de los puntos de venta que pudieran requerir investigación.

L.5	Canales digitales de venta y servicios interactivos	
L.5.1	**Sistemas digitales de juego**	
Objetivo:	Proteger la confidencialidad, integridad y disponibilidad de los sistemas digitales de juego con el objetivo de proteger los juegos y los datos de los jugadores.	
L.5.1.1	Arquitectura de sistemas por capas	*Control* La organización deberá implementar una arquitectura por capas para los sistemas digitales de juego a fin de garantizar la seguridad en el almacenamiento y el tratamiento de datos.
L.5.1.2	Ataques activos y pasivos	*Control* Se implementarán medidas adecuadas para detectar, prevenir y mitigar ataques técnicos comunes, tanto activos como pasivos, así como para responder a ellos. Asimismo, la organización acordará políticas de parches orientadas a sistemas digitales de juego, desarrollados y respaldados internamente o por terceros.
L.5.1.3	Segregación de redes	*Control* Las bases de datos de producción que contengan datos sobre jugadores o transacciones residirán en redes separadas de los servidores donde se alojen las páginas web.
L.5.1.4	Información de sesiones	*Control* El identificador de sesiones de los usuarios siempre se creará de manera aleatoria, en la memoria, y se suprimirá cuando finalice la sesión del usuario.
L.5.1.5	Identificación de puntos de entrada y salida	*Control* Se identificarán, gestionarán, seguirán y controlarán todos los puntos de entrada y salida a sistemas de redes abiertas al público. La organización controlará todos sus sistemas digitales de juego a fin de prevenir, detectar y mitigar ataques cibernéticos y responder a ellos.
L.5.1.6	Generación y almacenamiento de registros	*Control* Se generarán, y se conservarán por un período establecido, registros de seguridad predefinidos sobre cada componente sensible del sistema a fin de controlar y subsanar anomalías, fallos y alertas.
L.5.1.7	Pruebas de seguridad	*Control* Los cambios que se introduzcan en los sistemas más importantes se someterán a pruebas de seguridad adecuadas. Se realizarán pruebas regulares contra intrusiones, como mínimo anualmente, para tratar de evitar que se detecten y se aprovechen las vulnerabilidades y otros puntos débiles del sistema.
L.5.1.8	Divulgación responsable	*Control* El operador de lotería contará con una Política de divulgación responsable para la divulgación de las vulnerabilidades de seguridad por parte del público a la lotería.

L.5.2	Cuenta de jugador	
Objetivo:	Proteger al jugador y gestionar el riesgo de fraude y blanqueo de capitales.	
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.5.3	Diseño de juegos y aprobación	
Objetivo:	Garantizar que los diseños de los juegos cumplan las obligaciones legislativas y reglamentarias y cuenten con la correspondiente autorización antes de su activación.	
L.5.3.1	Documentación de los procedimientos de juego	*Control* Las normas establecidas abarcarán el diseño y el desarrollo. Además, los jugadores podrán acceder a las reglas de los juegos.
L.5.3.2	Aprobación y modificación de los juegos	*Control* Se definirá un procedimiento de aprobación para validar el control de cada juego nuevo y las modificaciones relevantes que se produzcan en los sistemas digitales de juego. Los diseños definitivos de los juegos deberán ser autorizados formalmente mediante un proceso en que participe la función de seguridad.

L.5.4	**Seguridad de los métodos de pago**	
Objetivo:	Proteger los métodos de pago de usos fraudulentos.	
L.5.4.1	Compilación de datos	*Control* La compilación de datos sensibles relacionados directamente con los pagos se limitará a datos estrictamente necesarios para cada transacción.
L.5.4.2	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.5.4.3	Autorización del servicio de pago	*Control* La organización verificará que el servicio de pago garantice la protección de los datos de los jugadores, donde se incluyen información personalmente identificable que facilite el jugador y datos sobre los pagos.
L.5.4.4	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	
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, así como las reglas correspondientes a todos los tipos de eventos deportivos autorizados y todos los tipos de apuestas autorizadas para cada deporte que se oferte, entre otros.

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 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 la actividad fraudulenta. 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 reducir al mínimo 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, 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 una cuantía determinada. 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 certificador.

L.7	Terminales de videolotería interactivos	
L.7.1	**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	Incidencias con VLT	*Control* Se documentarán procedimientos para gestionar disputas o reclamaciones de clientes con respecto a ganancias o pérdidas.
L.7.1.5	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.

Anexo C (controles «S»): controles para operadores y proveedores de sistemas de juego

Los controles «S» se aplican a los sistemas de juego, tal como se definen en este estándar, y deberán incluirse en el ámbito de certificación de la organización que desarrolle y/u opere el sistema de juego, se trate de un proveedor de tecnología o de los desarrolladores internos del operador.

S.1	**Garantía de seguridad de los sistemas de lotería**	
S.1.1	**Desarrollo de la seguridad en las aplicaciones de los sistemas de juego**	
Objetivo:	Garantizar la seguridad del diseño de los sistemas de lotería.	
S.1.1.1	Política de seguridad para el desarrollo de las aplicaciones	*Control* El proveedor de tecnología de lotería dispondrá de una política de seguridad para las aplicaciones durante todo el período de su desarrollo.
S.1.1.2	Análisis de código estáticos y dinámicos	*Control* El proveedor de tecnología de lotería realizará análisis de código estáticos y dinámicos, y entregará un resumen de los resultados al operador junto con las notas de lanzamiento de su producto a un entorno de producción. Este procedimiento se llevará a cabo tanto para el lanzamiento inicial a producción como para cualquier relanzamiento subsiguiente significativo.
S.1.1.3	Pruebas de seguridad	*Control* El proveedor de tecnología de lotería realizará pruebas de seguridad de sus productos y servicios, alojados y configurados de manera que muestren cómo el operador los implementará en un entorno de producción. Se entregará un resumen de los resultados al operador junto con las notas de lanzamiento de su producto a un entorno de producción. Este procedimiento se llevará a cabo tanto para el lanzamiento inicial a producción como para cualquier relanzamiento subsiguiente significativo.
S.1.1.4	Prácticas de codificación segura	*Control* El proveedor de tecnología de lotería establecerá un conjunto de prácticas de codificación segura que sus desarrolladores deberán seguir. Asimismo, aplicará medidas para controlar la efectividad y el cumplimiento de dichas prácticas.
S.1.1.5	Capacitación y concienciación en codificación segura	*Control* El proveedor de tecnología de lotería dispondrá de un programa de capacitación y concienciación en prácticas de codificación segura para todos los desarrolladores de códigos para sistemas de juego (tal como se define en este estándar).

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 lotería.	
S.1.2.1	Controles de integridad durante el proceso de desarrollo	*Control* El proveedor de tecnología de lotería garantizará la integridad de los programas y controladores que desarrolle en cada etapa del proceso de desarrollo, incluido al menos, durante el proceso de control de calidad y de implementación de los programas y controladores en el entorno de producción, entre otros.
S.1.2.2	Registro de seguridad	*Control* El proveedor de tecnología de lotería se asegurará de proporcionar los registros de seguridad adecuados de los programas/controladores que desarrolle al equipo de seguridad de la organización de lotería para que los integre a las herramientas de seguridad de la organización a fin de garantizar la integridad de sus programas/controladores. El proveedor de tecnología de lotería proporcionará al equipo de seguridad un documento que explique cómo interpretar el registro de seguridad.
S.1.2.3	Integridad de los archivos	*Control* El proveedor de tecnología de lotería identificará y documentará archivos críticos en sus productos a fin de que el operador de lotería verifique la integridad del entorno de producción.
S.1.2.4	Integridad de los equipos	*Control* El proveedor de tecnología de lotería adoptará 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 lotería. En este contexto, los equipos incluyen como mínimo, los terminales de videolotería, los equipos del punto de venta de lotería, 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* El proveedor de tecnología de lotería garantizará que dispone de un proceso para actualizar de manera oportuna los programas/controladores y cualquier biblioteca de códigos externa que 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 lotería, así como las consideraciones comerciales.
S.1.2.6	Divulgación responsable	*Control* El proveedor de tecnología de lotería pondrá a disposición de las organizaciones 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 seguridad 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 obligaciones de la lotería con las especificaciones del proveedor.	
S.1.3.1.1	Obligaciones para juegos instantáneos	*Control* El proveedor validará formalmente las obligaciones con la lotería y los traducirá en especificaciones; cualquier cambio en las especificaciones seguirá el proceso de gestión de cambios tanto de la lotería 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 los juegos instantáneos está sujeto a la aplicación de los controles contemplados en la sección L.2.4 del SCS de la WLA sobre los sorteos de lotería electrónicos y los juegos instantáneos y a los requisitos acordados entre el operador y el proveedor.
S.1.3.2.2	Validación de los datos de juego	*Control* El proveedor garantizará que un equipo independiente valide los datos lógicos del juego con los requisitos de la lotería. Los informes con los resultados se pondrán a disposición de la lotería.
S.1.3.2.3	Confidencialidad de los datos	*Control* El proveedor 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 proveedor validará formalmente con la lotería los textos e imágenes finales de los boletos antes de su impresión.
S.1.3.3.2	Pruebas de integridad	*Control* El proveedor 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 requerida de premios.
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 a la organización de lotería.

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 las 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.2.4.3 del SCS de la WLA titulado «Verificación de la aleatoriedad y la 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 del SCS de la WLA «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 y la 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 configurarán de manera que notifiquen a los administradores locales.