CONSEJO NACIONAL DE JUEGOS DE SUERTE Y AZAR

BORRADOR

Anexo Técnico
Lotería Instantánea

Octubre 31 de 2013
VERSIÓN 1

Este documento es confidencial y sólo podrá ser conocido con autorización explícita del Consejo Nacional de Juegos de Suerte y Azar-CNJSA.

CONTENIDO

MARCO LEGAL 3
GLOSARIO-TÉRMINOS-DEFINICIONES 4
OBJETIVO 7
1. ASPECTOS TÉCNICOS GENERALES 8
1.1. REQUISITOS FUNCIONALES, TECNOLÓGICOS Y LOGÍSTICOS DE FUNCIONALIDAD DEL SISTEMA CENTRAL DEL JUEGO - SCJ. 12
1.2. REQUISITOS GENERALES DE FUNCIONALIDAD DE IMPRESIÓN DE LOS BOLTEOS INCLUYENDO LA RIFA PREVIA A TRAVÈS DE UN GENERADOR DEL NÚMERO ALEATORIO 15
1.3. ESPECIFICACIONES TECNICAS PARA LA IMPRESION DE TIQUETES DE JUEGOS DE RESOLUCION INSTANTANEA 16
1.3.1. Especificaciones de los tiquetes 16
1.3.2. Protocolos de prueba de tiquetes 19
1.4. REQUISITOS GENERALES DE LA TERMINAL DE VENTA - TDV 19
1.4.1. Requisitos de Identificación física de las terminales de venta 20
1.5. REQUISITOS GENERALES PARA LA COMUNICACIÓN 21
1.5.1. Requisitos para los protocolos de comunicación 21
1.5.2. Pérdida de comunicación. 21
2. REQUISITOS TECNOLÓGICOS DEL SISTEMA CENTRAL DEL JUEGO – SCJ. 22
2.1. BATERIA DE RESERVA 22
2.3. BASE DE DATOS DEL SISTEMA CENTRAL DEL JUEGO 22
2.3.1. Acceso a la base de datos 22
2.3.2. Información almacenada en la base de datos 22
2.4. ESTACIONES DE TRABAJO DEL SCJ 24
3. REQUISITOS DE SEGURIDAD 25
3.2 CONTROL DE ACCESO 27
3.3 SEGURIDAD EN EL SISTEMA DE COMUNICACIÓN 28
3.4 SEGURIDAD EN EL ACCESO REMOTO 28
3.5 ALTERACIÓN DE DATOS 29
3.6 LAS COPIAS DE RESPALDO Y RECUPERACIÓN 29
3.7 REQUISITOS PARA LA RECUPERACIÓN 29
3.8 REGISTRO, TRAZABILIDAD DE LAS OPERACIONES DE JUEGO Y LA BASE DE DATOS. 30
3.9 CONTINUIDAD DE LA ACTIVIDAD DE JUEGO 30
4. ASPECTOS ADMINISTRATIVOS 31
5. CERTIFICACIÓN 31

MARCO LEGAL

El artículo 1° de la Ley 643 de 2001 definió que el monopolio regulado en dicha normatividad, es la facultad exclusiva del Estado para explotar, organizar, administrar, operar, controlar, fiscalizar, regular y vigilar todas las modalidades de juegos de suerte y azar, y para establecer las condiciones en las cuales los particulares pueden operarlos, facultad que siempre se debe ejercer como actividad que debe respetar el interés público y social y con fines de arbitrio rentístico a favor de los servicios de salud, incluidos sus costos prestacionales y la investigación.

En sesión llevada a cabo el día DIA del mes de MES de 2012, el Consejo Nacional de Juegos de Suerte y Azar, en cumplimiento …… aprobó el reglamento del juego denominado Lotería Instantánea, decisión que consta en el acta No. NÚMERO.

GLOSARIO-TÉRMINOS-DEFINICIONES

a) **Administrador del juego:** ente público que agremia a los Departamentos y al Distrito Capital y escogido por éstos para seleccionar al operador del juego, supervisar el contrato, aprobar las emisiones y el plan de premios, así como para recaudar las rentas y fiscalizarlas

b) **Algoritmo:** conjunto prescrito de instrucciones o reglas bien definidas, ordenadas y finitas que permite realizar una actividad mediante pasos sucesivos que no generen dudas a quien deba realizar dicha actividad al sistema computacional en el que se apliquen.

c) **Apuesta:** Es el precio que paga el jugador por tener el derecho a participar en el sorteo. Para todos los efectos se considerará que existe una apuesta válida, cuando la transacción es procesada y registrada por el sistema del juego.

d) **Área de juego:** zona del tiquete en la que permanece ocultos símbolos o números que determinan el posible premio, la cual debe ser raspada para develar si el tiquete es ganador o no

e) **Emisión:** cantidad determinada de tiquetes de lotería instantánea asociada a un único pre sorteo, con características individuales tales como: nombre comercial, fecha de inicio, cantidad de tiquetes impresos, plan de premios, número consecutivo, entre otros

f) **En línea**: expresión que se utiliza para denotar que un elemento se encuentra conectado o hace parte en forma permanente de un sistema de información. La operación en línea implica además, que los programas se ejecutan de tal forma que los datos se actualizan de inmediato en los archivos del sistema.

g) **Lector de códigos**: dispositivo electrónico utilizado en los puntos de venta para descifrar el código que identifica el tiquete y reportar al sistema central del juego la información tanto de los tiquetes vendidos como de los premiados.

h) **Medios de comunicación:** Instrumento o forma de contenido por el cual se informa a los apostadores, y al público en general, las novedades relacionadas con el juego como inicio y cierre de emisiones y premios entregados, entre otros.

i) **Página Web:** información electrónica conformada por páginas con hiperenlaces a la cual se puede acceder desde un navegador y está almacenada en un servidor remoto y con acceso al público.

j) **Premios mayores:** aquellos premios de gran valor cuya frecuencia por emisión es baja, los cuales estarán claramente definidos en cada emisión.

k) Premios menores: aquellos premios de pequeño valor cuya frecuencia por emisión es alta, los cuales estarán claramente definidos en cada emisión.

l) Punto de venta: lugar donde se comercializa el juego y se paga el premio al jugador, el cual debe estar conectado en línea y tiempo real con el Sistema Central del Juego y debe ser autorizado por el operador

m) Registro Informático: tipo o conjunto de datos almacenados en un sistema de información con un propósito específico.

n) Sistema Central del Juego: plataforma tecnológica que soporta el juego la cual está compuesta por los equipos (*hardware*) requeridos y el conjunto de programas (*software*) que garantizan la adecuada operación del juego, y el envío de la información solicitada por el administrador del juego para efectos de control. Debe disponer de mecanismos de autenticación de las terminales de venta; garantizar la confidencialidad e integridad en las comunicaciones; validación, procesamiento y almacenamiento de la activación y venta de tiquetes y el pago de premios

o) Sistema de Comunicación: medio para transmitir información relacionada y validada, que hace parte del Sistema Central del Juego, el cual permite la interacción ininterrumpida entre los puntos de venta, la entidad fiduciaria, el centro de cómputo del administrador del juego, y todos las personas jurídicas y naturales involucradas en la operación y control del juego

p) Software de Control: componente del Sistema Central del Juego que permite el procesamiento y validación, en línea y tiempo real, de la información transaccional que se intercambia entre éste y las terminales de los puntos de venta.

q) Tiempo real: expresión que se utiliza en los sistemas informáticos para indicar que tienen capacidad de sincronizar en intervalos de tiempo bien definidos, el funcionamiento del sistema en simultánea con las acciones que se presentan en el mundo físico.

r) Tier III. por su sigla en inglés *"Telecomunications Infraestructure Standard for Data Centers"* corresponde al nivel de fiabilidad que debe tener un centro de cómputo de acuerdo con las características del negocio. Existen cuatro niveles Tier, donde a mayor número, mayor disponibilidad tendrá el centro de cómputo. Tier III opera con una disponibilidad del 99.982%, lo que significa que la infraestructura garantiza que el sistema no fallará más de 1.6 horas al año y que no habrá interrupciones por mantenimientos planificados

s) Tiquete: documento al portador pre impreso especialmente diseñado para que el jugador pueda participar de forma inmediata en el juego, raspando o arrancando una película o capa de seguridad que recubre parte del tiquete, y bajo la cual se halla el resultado de la apuesta, que de acuerdo a sus características de seguridad permite su validación en línea y tiempo real por el Sistema Central del Juego

t) Tiempo real: sistema digital que interactúa activamente con un entorno con dinámica conocida en relación con sus entradas, salidas y restricciones temporales, para darle un correcto funcionamiento de acuerdo con los conceptos de predictibilidad, estabilidad, controlabilidad y alcanzabilidad.

u) Valor de la Emisión: resultado de multiplicar el número de tiquetes que componen la emisión por el precio de venta al público. Sobre este valor descontando el IVA se determina el porcentaje autorizado para el plan de premios.

OBJETIVO

Este documento establece los requisitos técnicos mínimos de la lotería instantánea, que deben ser cumplidos por el Operador.

La determinación de los requisitos y condiciones, por su condición fundamentalmente tecnológica, pueden estar sujetas a cambios como consecuencia del desarrollo de la tecnología. Para la elaboración de este documento, se ha tenido en cuenta la información en materia de normas, estándares y reglamentaciones técnicas Internacionales, en caso que alguna de estas normas técnicas internacionales quedara en desuso, se debe utilizar cualquier otra norma que la reemplace.

Los nuevos desarrollos en la tecnología y los requerimientos adicionales que el Operador solicite a los fabricantes deberán ser compatibles con los requisitos mínimos contemplados en este documento.

Este documento no contempla las especificaciones técnicas y requerimientos para el envío de la información solicitada por el administrador del juego.

1. ASPECTOS TÉCNICOS GENERALES

El sistema de la lotería instantánea consta de las siguientes actividades generales que determinan los aspectos técnicos:

1. Definición de la emisión
2. Pre-sorteo e impresión de los tiquetes
3. Distribución logística de los tiquetes
4. Activación en el punto de venta de los paquetes de tiquetes
5. Validación de los tiquetes premiados y pago de premios
6. Cierre de la emisión

El operador deberá garantizar el conjunto de sistemas e instrumentos técnicos o telemáticos, que posibiliten la organización, impresión, comercialización y ejecución de estas actividades; deberá disponer de los mecanismos suficientes para garantizar, entre otros, la confidencialidad e integridad en las comunicaciones, validación, autenticidad y cómputo de los tiquetes, el control de su correcto funcionamiento y el acceso a los componentes del sistema informático exclusivamente del personal autorizado del administrador del juego en las condiciones que este pudiera establecer.

El operador una vez defina una emisión y cuente con todas las aprobaciones necesarias, deberá enviar al administrador del juego la data con la información de fecha de inicio, fecha final prevista, número de tiquetes, zonas del país donde será distribuida, número de tiquetes premiados, valor total en premios y toda aquella información que el administrador del juego considere conveniente solicitar. Cabe anotar, que esta información corresponde a la parte técnica de la operación del juego y es aparte de la información que puede ser requerida por el área financiera del administrador del juego para validar la emisión de la lotería.

Una vez definida la emisión de tiquetes el operador deberá garantizar que el impresor seleccionado realice por un sorteo aleatorio que defina la impresión de los tiquetes ganadores, para lo cual el impresor deberá estar certificado con las normas de seguridad utilizadas en la industria para una impresión de estas características. El tiquete tiene dos identificadores, el número del tiquete que es visible y se utiliza para la identificación y distribución logística de los tiquetes, y el código oculto del tiquete que lo valida como ganador. Una vez impresos los tiquetes con sus códigos ganadores por emisión, se deberá generar una copia encriptada de los archivos con esta información y enviarla al administrador del juego, sin la clave de desencriptación. El operador en cambio, deberá tener acceso a la información del número y códigos de cada tiquete para poder controlar tanto la distribución como los tiquetes premiados.

Cuando se dé por finalizada la emisión ya sea porque se cumplió la fecha estimada para el sorteo o porque el operador considere conveniente finalizar anticipadamente la emisión (y cumpla los requisitos estipulados para la cancelación anticipada), el operador debe entregarle al administrador del juego la clave de desencriptación para que este realice en sus instalaciones el escrutinio

El operador deberá entregarle al administrador del juego tanto el hardware como software requerido para realizar el escrutinio, con todas las licencias necesarias de bases de datos, sistema operativo y demás. A su vez, el operador será el encargado de proveer el canal de comunicación entre su centro de cómputo y el definido por el administrador del juego para recibir la data. Es responsabilidad del operador enviar oportunamente toda la información necesaria al administrador del juego.

La distribución logística de los grupos de tiquetes pre impresos a los puntos de venta deberá ser controlada por el operador de acuerdo a la numeración visible del tiquete, que es diferente del código que se asigna a los tiquetes ganadores. No debe existir ninguna forma de relacionar la numeración del tiquete con el código ganador, esto con el objetivo de que durante el tiempo del sorteo no sea posible identificar dónde se encuentran los tiquetes ganadores. El operador debe garantizar las medidas de seguridad de todo este proceso.

La información correspondiente a la distribución de los tiquetes por punto de venta debe ser reportada por el operador al administrador del juego, para ser almacenada en una base de datos que le permita realizar análisis de distribución geográfica, del mercado y minería de datos en general.

El punto de venta podrá activar por grupos de tiquetes, o por tiquete individual, según lo considere conveniente y en acuerdo con el operador. Cuando se active el tiquete o el grupo de tiquetes, la validación se realiza mediante la conexión al sistema central del juego del operador donde se captura la información del (los) número(s) de tiquete(s) que pasa(n) a estar activo(s), el operador debe validar esta información con el reparto logístico de los tiquetes y si la emisión se encuentra activa. La data de la transacción, que incluye la activación y validación debe ser copiada al servidor del administrador del juego. Todo tiquete activado se considera que está jugando y causa derechos de explotación que deberán ser transferidos a la salud.

Cuando el jugador detecte un tiquete ganador, el premio debe ser validado por el punto de venta a través el código del premio mediante una conexión con el sistema central de juego del Operador, y esta transacción transmitida en línea y tiempo real al administrador del juego.

El operador debe disponer del material de software, equipos, sistemas, terminales e instrumentos en general, necesarios para el desarrollo de las actividades de juego; debidamente certificados, correspondiendo al operador la certificación de los sistemas técnicos de juego y el establecimiento de las especificaciones necesarias para su funcionamiento.

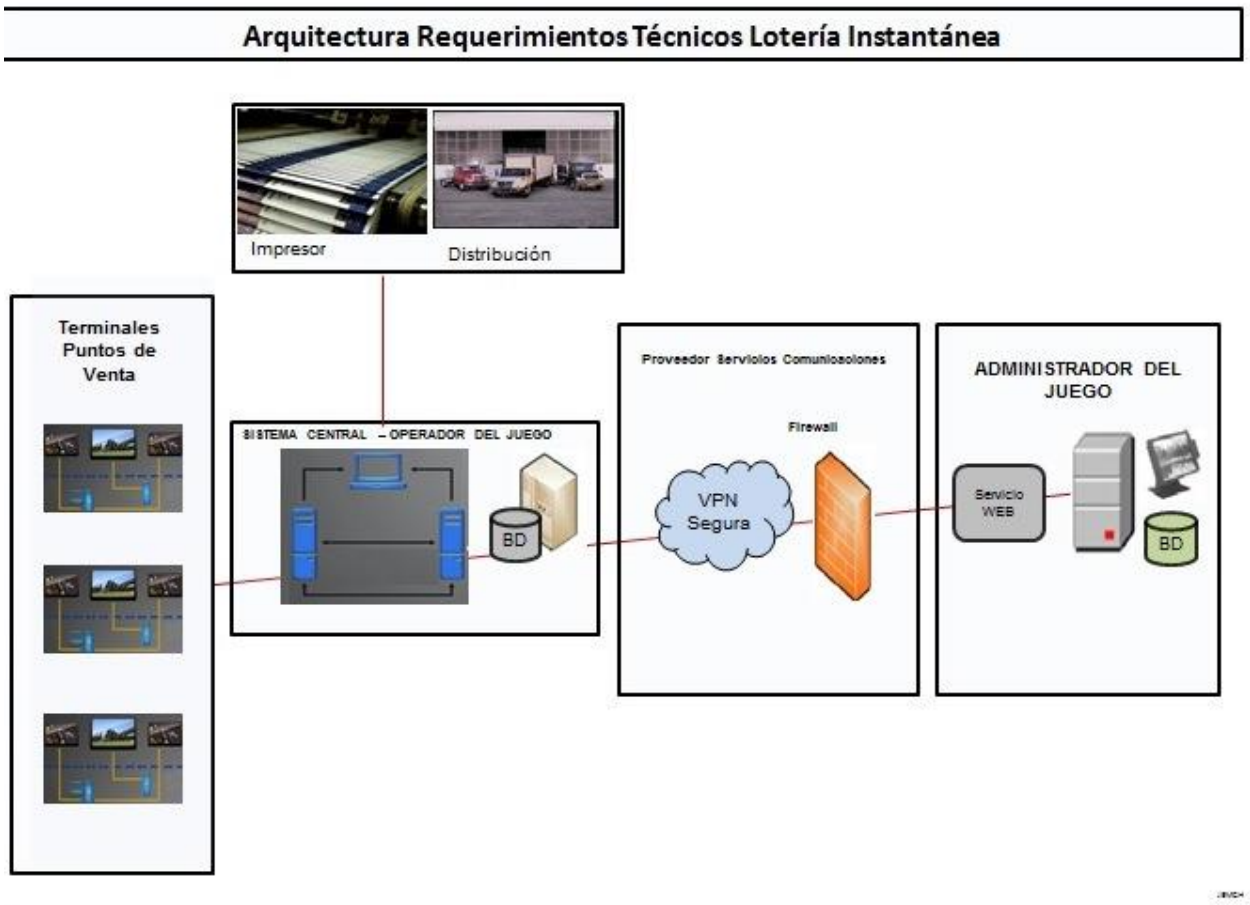
Los sistemas técnicos de juego empleados por el Operador habilitado para la organización, explotación y desarrollo de las actividades de juego por medios electrónicos, informáticos, telemáticos e interactivos reunirán las condiciones que, mediante disposición, establezca el CNJSA y deberán permitir el cumplimiento de las obligaciones establecidas en la Ley.

El sistema central del juego deberá incluir

1. Servidores Centrales, conjunto de servidores con altos niveles de seguridad y redundancia ubicados en el centro de cómputo del operador donde se almacenan:
    a. Los resultados de la impresión de los tiquetes ganadores identificados por el número oculto, una vez se cierre la emisión.
    b. La distribución de los tiquetes en los puntos de venta por número visible del tiquete.
    c. La activación de los tiquetes en los puntos de venta por el software de control del juego.
    d. La confirmación de los premios realizada por el software de control del juego.
    e. La generación de bases de datos transaccionales, sistemas de respaldo y en general todo componente informático encargado de garantizar la operación del juego.
2. Software de Control del Juego, software encargado de las validaciones de los tiquetes en el punto de la venta y la validación de los premios ganadores en cada tiquete contra la base de datos de la impresión de los tiquetes.
3. El Sistema de Comunicación, permite la interacción ininterrumpida entre el centro de cómputo central, las terminales de puntos de venta, el centro de cómputo alterno, el administrador del juego, y todos los entes involucrados en la operación y control del juego.
4. Lector de código, componente de las terminales en los puntos de venta, utilizado para agilizar la transmisión de la información de los tiquetes vendidos al sistema central.
5. Página web oficial del juego, página de promoción y divulgación de la información pertinente para informar a los apostadores y al público en general situaciones y/o eventos relacionados con cualquier aspecto relacionado con el juego.

Este subsistema debe disponer de los mecanismos suficientes para garantizar, entre otros, la identificación y autenticación digital de las terminales de ventas, la comprobación de la autenticidad del tiquete y del premio, la confidencialidad e integridad en las comunicaciones. Toda transacción de validación o pago de premio además de ser validada por el sistema debe ser reportado en línea y tiempo real al administrador del juego. Será responsabilidad del Operador garantizar la funcionalidad necesaria para la operatividad y respaldo del juego.

El siguiente diagrama muestra en forma genérica su arquitectura:



La administración y correcto funcionamiento de la plataforma tecnológica y sistemas de información que el operador debe haber suministrado al administrador del juego para recibir y procesar la información requerida para el control del juego, estará a cargo del administrador del juego. Dentro de estos sistemas de información se incluye el todo el software base y el software requerido para realizar el escrutinio. El Operador se encargará de proveer al administrador del juego del canal de comunicación para la transmisión en línea y tiempo real de una réplica de la data transaccional generada por la operación del juego tanto en cuanto a activación y validación de tiquetes, como a la validación y pago de premios.

La administración, correcto funcionamiento, cumplimiento de normas, estándares y reglamentaciones técnicas, de la plataforma tecnológica y sistemas de información del Operador, estará a cargo del Operador autorizado por el administrador del juego, quién dispondrá y responderá por el software, equipos, sistemas, terminales e instrumentos en general necesarios para garantizar el funcionamiento del sistema.

El Operador a partir de la información detallada de la impresión, distribución, validaciones y premios de tiquetes entregada por las terminales de ventas, almacenada en el Sistema Central del Juego, en adelante “SCJ”, generará los informes administrativos y control solicitadas por el administrador del juego.

El envío de la información encriptada de los premios con su código oculto, deberá ser enviada al administrador del juego por el Operador antes de iniciar la activación de un tiquete de esa emisión, en un medio electrónico (DVD, CD, etc.) que garantice la seguridad de la información y su imposibilidad de ser leída antes del cierre de la emisión. De igual manera, el envío de la información de la distribución de los tiquetes de acuerdo a su número visible en los diferentes establecimientos del país, deberá ser suministrada al administrador del juego antes de permitirse su activación en los puntos de ventas. El envío de la data transaccional de activación y pago de premios en cualquier punto de venta al administrador del juego deberá ser enviada en línea y tiempo real a través de la red de comunicaciones establecida por el Operador.

Las especificaciones técnicas y requerimientos para el envío de la información indicada en el presente documento por medio de un servicio web al administrador del juego, será indicada a nivel de detalle de trama por parte del administrador del juego al Operador seleccionado mediante un documento de Especificaciones Técnicas y requerimientos para el envío de información por parte del Operador.

1.1. REQUISITOS FUNCIONALES, TECNOLÓGICOS Y LOGÍSTICOS DE FUNCIONALIDAD DEL SISTEMA CENTRAL DEL JUEGO - SCJ.

El juego debe ser operado sobre una plataforma tecnológica a cargo del operador, que funciones en línea y en tiempo real, y cuya capacidad transaccional cumpla con los requerimientos necesarios para la operación de este tipo de juego. Todas las operaciones transaccionales: activación del tiquete, reporte de la venta de tiquetes, y de pago de premios, deben quedar registradas de inmediato en esta plataforma y con una copia espejo enviada al administrador del juego.

La administración del sistema central del juego debe incluir la generación de reportes periódicos determinados por el administrador del juego, que permitan el monitoreo constante de la rotación del producto, finalización de emisión, lanzamiento de nuevas emisiones, distribución geográfica de los tiquetes y los premios, entre otras.

Los componentes del SCJ son además de los elementos de hardware requeridos, un conjunto de programas (software) que garantizan la adecuada operación del juego. A su vez, esta plataforma tecnológica es la encargada del envío de la información de forma oportuna al administrador del juego, o sea en bloque o *batch* para los datos de la impresión de los tiquetes y su distribución en los puntos de venta, y en línea y tiempo real para las activaciones o validaciones del tiquete y la validación de los premios.

El Sistema Central del Juego deberá tener una infraestructura tecnológica estable que se garantice la disponibilidad de la información almacenada en las bases de datos: información de control, distribución de los tiquetes, tiquetes activados – validados y tiquetes ganadores. Los servidores que lo componen deberán cumplir con los requerimientos de conectividad y seguridad (se refiere a los estándares IEEE 802 y 27001); y tener como mínimo:

- Infraestructura para alojar el aplicativo local (ubicado en donde el administrador del juego lo designe), que será espejo del sistema que se utilizará para administrar la lógica del juego, el cual debe tener como mínimo las siguientes características:
    - *Frontend* en ambiente web.
    - Módulo de administración de usuarios.
    - Módulo de reportes financieros, de ventas, de novedades de premios, estadísticos, escrutinio de premios.
    - Base de datos relacional.
    - Servidores *blade*, con fuente, y discos redundantes
- Manuales de sistema y de usuario
- Implementar los servicios de sincronización que se requieran con los contenedores de bases datos locales del administrador del juego
- Canal de comunicaciones con su respectiva redundancia.
- Implementar directamente o gestionar la instalación, en el lugar que el administrador del juego lo indique, las condiciones eléctricas y su soporte, necesaria para la correcta operación de la infraestructura espejo del sistema de gestión del juego, que será entregada por el operador al administrador del juego.

Las instalaciones del Sistema Central del Juego deberán estar ubicadas en la república de Colombia así como las del sistema de respaldo; ambos, estarán en instalaciones sujetas, en todo momento, a control de acceso y vigilancia, siendo el Operador el responsable de su custodia.

El Sistema Central del Juego debe permitir:

- Registrar todas las transacciones y operaciones de juego realizadas desde las terminales de los puntos venta conectadas al SCJ, activaciones y validaciones de tiquetes ganadores, datos de control, así como eventos de funcionamiento del juego;
- Garantizar el correcto funcionamiento de las actividades de juego;
- Cruzar el plan de distribución logística con la distribución física de los tiquetes.
- Comprobar en todo momento las operaciones realizadas, así como reconstruir de manera fiable todas las transacciones u operaciones realizadas a través del SCJ
- Generar informes gerenciales sobre el resultado de la emisión y el retorno al jugador teórico vs práctico.
- Generar informes del cruce de los tiquetes ganadores vs el informe del impresor una vez sea cerrada la emisión.
- El Operador facilitará el acceso y total colaboración a los inspectores del administrador del juego a las instalaciones del SCJ para posible inspección, con independencia del lugar de su ubicación y del personal que preste servicios en las instalaciones del Operador, sea propio, sea de las entidades que le faciliten o provean algún tipo de servicio. El Operador será responsable de la falta de colaboración del citado personal, con independencia de la relación jurídica o laboral que le vincule.

El Operador deberá presentar ante solicitud del administrador del juego, la documentación y herramientas de hardware/software que permiten realizar pruebas en los módulos del software.

El SCJ debe cumplir los siguientes aspectos técnicos mínimos, cuya validación será realizada por un tercero:

- Contar con un programa aplicativo que permita desde una estación de trabajo, realizar una búsqueda exhaustiva en línea de un registro de sucesos significativos ocurridos en el día o con anterioridad a éste, de la información registrada en la base de datos.
- Capacidad para interconectar múltiples terminales de ventas.
- Capacidad para parametrizar las reglas de negocio básicas para la operación general del sistema, tales como: perfiles, usuarios, activaciones y eventos.
- Capacidad de registrar las transacciones financieras que se generan durante la operación para el cálculo de las ventas diarias durante un rango de tiempo.
- Generación de la información de las activaciones y premios pagados, con corte en el cierre de operación para el reporte automático de resultados por establecimiento y terminal.
- Capacidad de registrar todas las activaciones de tiquetes y premios pagados en línea, mediante conexión de las terminales de venta.
- Asegurar la existencia de información diaria y mensual para control contable de las terminales de ventas.
- Mantener un log de las validaciones de tiquetes y pagos de premios ocurridos en las bases de datos.
- Posibilidad de verificar el pago de premios por terminal de venta.
- Implementar procedimientos que permitan realizar un control de versiones de los programas, archivos, tablas, repositorios, configuraciones, etc.
- El software que opere el SCJ debe contar con una certificación de un laboratorio autorizado por la Secretaria Técnica - COLJUEGOS sobre el cumplimiento de estos requerimientos técnicos y asígnale firmas digitales al código ejecutable del *software*, ya sea con una clave propia o por una entidad de autenticación certificada.

Fallas en la Comunicación:

Las fallas de comunicación entre las Terminales de Venta y el Sistema Central del Juego imposibilitan la activación de los tiquetes y el pago de premios. El Punto de Venta solo está autorizado a vender tiquetes que se encuentren validados con el SCJ, en el caso de que el Operador permita al punto de venta realizar la activación de paquetes de tiquetes, el Punto de Venta podrá vender aquellos tiquetes que previamente hayan sido validados y activados. El pago de eventuales tiquetes premiados quedará aplazado hasta el momento en que se haya superado la contingencia para poder validar el premio, y reportar la transacción correspondiente al pago del premio.

En caso de fallas en la comunicación entre alguna terminal de venta y el Sistema Central del Juego, el Operador deberá contar con un plan de contingencia que garantice la reanudación de

la correcta operación del juego en esa terminal en un término no mayor a 24 horas desde la ocurrencia del hecho.

Fallas en el Funcionamiento del Software:

En cualquier momento en que se llegare a detectar eventuales fallas en el funcionamiento del software de control, que pudiera afectar y/o alterar la confiabilidad de las informaciones, activaciones, validaciones, etc. del juego, el operador dispondrá de inmediato la suspensión provisional de la venta de tiquetes, del pago de premios y de cualesquiera otras actividades propias de la mecánica de desarrollo del juego.

La suspensión así determinada se mantendrá vigente hasta tanto la misma sea superada totalmente, de acuerdo a los protocolos previamente establecidos para este fin por el Operador y avalados por el administrador del juego.

Si evaluada técnicamente la magnitud de la contingencia, el operador establece que la duración de la misma será mayor o igual a 24 horas, el Operador dispondrá lo necesario para dar publicidad a tal hecho por medios de comunicación masivos, dentro de las primeras horas de ocurrencia del evento

1.2. REQUISITOS GENERALES DE FUNCIONALIDAD DE IMPRESIÓN DE LOS BOLTEOS INCLUYENDO LA RIFA PREVIA A TRAVÈS DE UN GENERADOR DEL NÚMERO ALEATORIO

El impresor mediante un generador de números aleatorios que garantice la trasparencia, realizará un sorteo previo para determinar los tiquetes ganadores. Este generador de número aleatorio deberá ser estadísticamente independiente, impredecible y pasar las pruebas realizadas por un laboratorio certificador que garanticen la aleatoriedad de los resultados que se imprimen en los tiquetes. El Operador deberá presentar al administrador del juego la certificación otorgada por un laboratorio certificador avalado por la Secretaría Técnica - Coljuegos sobre la calidad del proceso de impresión que realiza. El administrador del juego se reserva el derecho de solicitar con frecuencia dicha certificación.

Los tiquetes ganadores serán identificados con un código oculto. El impresor deberá enviar al Operador dicha información a través de un archivo encriptado para que mediante el Sistema Central del Juego sea posible validar los tiquetes ganadores a través de las terminales de venta. Ese mismo archivo encriptado, deberá ser enviado al Administrador del Juego, pero la llave de descriptación solo será entregada una vez finalice la emisión de la lotería.

1.3. ESPECIFICACIONES TECNICAS PARA LA IMPRESION DE TIQUETES DE JUEGOS DE RESOLUCION INSTANTANEA

1.3.1. Especificaciones de los tiquetes

Papel: Los tiquetes deberán ser impresos en papel virgen, reciclable, de 10 puntos satinado en un lado, del tipo para tiquetes de lotería instantánea, el cual deberá tener como mínimo las siguientes especificaciones:

- Calibre: 0.010 pulgadas o 254 micras
- Gramaje: 180 gramos por metro cuadrado
- Humedad: 5.5%
- Satinado: 50 unidades de satinado – 75 grados

El operador podrá ofrecer papeles de mayor calidad.

a. Cara Frontal del tiquete

Tintas: mínimo 4 tintas. Se deben usar tintas que resistan contacto con agua, jabones comerciales y otras condiciones normales del medio ambiente (humedad, alta y bajas temperaturas, entre otros).

Barniz:

- Sobre el 100% de la zona de impresión variable. Las películas de barniz deberán ser biodegradables, de base orgánica o, en última instancia, reciclables, no tóxicas.
- Los datos del juego bajo la capa de barniz, deben estar protegidos contra alteraciones o daño al momento de descubrir o raspar el área de juego.
- Sobre el 100% del arte del tiquete omitiendo el área correspondiente al juego cubierta por látex.

Patrones Benday:

- Los tiquetes deberán tener impreso un patrón de Benday (líneas curvas que cruzan el área de juego) en las áreas de juego del tiquete.
- Dentro de cada pliego de impresión se deberán emplear patrones Benday distintos para cada tiquete.
- Cada símbolo de juego deberá cruzar al menos una línea del patrón.

Ejemplo del patrón:



Color del área de Juego: La información variable que aparece en las áreas de juego del tiquete se imprimirá sobre un fondo de color que garantice la seguridad de la información variable impresa sobre de ella, sin afectar la legibilidad de la misma.

Colores de Bajo impresión: El tinte o color de base, deberá ser lo suficientemente claro para que los datos variables de juego sean flexibles, pero lo suficientemente coloridos para brindar un buen contraste con los colores de sobre impresión que ayuden a evitar posibles atentados al tiquete.

Capa de látex: Deberá colocarse una capa desprendible, ya sea de látex o cualquier otro material expuesto, sobre el barniz transparente para cubrir el área protegida correspondiente a los números y caracteres variables (premios y códigos de validación).

Sobreimpresión mínimo 5 tintas sobre fondo blanco (el blanco no cuenta como tinta). Con calidad fotográfica sobre el látex.

El material de raspar deberá ser opaco, de elastómero y deberá tener mínimo la calidad necesaria para:

- Impedir ver los números o figuras impresas debajo del área cubierta por este material ya sea por medios físicos, mecánicos, eléctricos o electrónicos o de cualquier otra índole.
- Asegurar su adherencia y permanencia sobre la superficie del tiquete.
- Imposibilitar el “levantar” y “reponer” la capa de látex ya sea por medios físicos y/o mecánicos.
- No dañarse por motivos meteorológicos
- Verse liso y sentirse suave al tacto.
- Ser fácilmente removible con un grado de resistencia razonable al ser raspado con artículos comúnmente utilizados para este fin, típicamente monedas. Se sugiere que la capa se pueda remover con tolerancias entre 25 y 75 gramos de presión
- Al removerse, el material se fragmente sin producir polvo.
- No causar irritación química o dermatológica alguna.
- Resistir al manejo normal de envío y distribución de los paquetes de tiquetes y manipulación de los mismos.

El material de raspar deberá:

- Aplicarse sobre el área de despliegue, cubriendo por completo el área del juego, sin rebasar el borde de sobreimpresión.
- Estar definido y uniforme el borde entre el área de raspar y la parte descubierta del tiquete.

Datos Sobre el área de juego:

La impresión de los datos sobre área de juego deberá hacerse por medio de una impresora de imágenes controlada por computadora con una resolución mínima de 240 dpi (puntos por pulgada). La impresión deberá cumplir con las siguientes características

- Se deberá hacer con tintas que no permitan la alteración o falsificación de los tiquetes.
- La tinta no se deberá alterar durante el proceso de remoción del material de raspar al aplicar una presión normal.
- No deberá existir transferencia de tintas del anverso al reverso de los tiquetes o en páginas adyacentes y viceversa, por haber sido enrollados o apilados en hojas durante la impresión o el acabado final.
- Tanto el área de datos variables, como el área de seguridad, serán zonas cubiertas de acuerdo a lo descripto en los puntos específicos.
- La(s) capa(s) deberá(n) estar libre(s) de vacíos y rayas detectables a simple vista y no tendrán huecos o marcas que dificulten la detección de tiquetes falsificados.
- La impresión de los datos e imágenes deberá ser clara, legible y no se deberá correr o distorsionar.
- Los datos variables impresos deberán estar perfectamente cubiertos por el material de raspar.

Troquelado: Entre cada tiquete, a lo largo del borde horizontal, debe existir la posibilidad de incluir micro perforaciones que permitan separar los tiquetes una vez impresos

b. Reverso del tiquete

Información: Al reverso del tiquete se imprimirá como mínimo la información descrita en el reglamento del juego
Tintas: A un (1) color: negro.

Código de inventario. Código de Inventario: Deberá estar al reverso del tiquete y debe contener como mínimo:

- 3 dígitos correspondientes al número de juego
- 6 dígitos del número de paquete
- 3 dígitos del número de tiquete.

El tiquete debe contener un código que tenga el número del tiquete, el cual es visible y se utiliza para la identificación y distribución logística de los tiquetes, y un código oculto del tiquete que lo valida como ganador.

Durante el proceso de impresión, el operador deberá asegurar la generación de un número que permita identificar como mínimo: el número de la emisión, el lote, la serie y la secuencia de los tiquetes, que estarán a disposición del administrador en caso de ser requeridos

1.3.2. Protocolos de prueba de tiquetes

Para asegurar la integridad y seguridad del tiquete, el operador a solicitud del administrador del juego, deberá presentar el resultado de las siguientes pruebas, que los tiquetes en su proceso de impresión deberán cumplir, y cuyo propósito se enuncia a continuación:

a) La prueba de Scratch -o latex- capa seguridad: determinar la cantidad de fuerza necesaria para quitar la seguridad rascar capa.
b) Las mediciones de código de barras: determinar que la calidad de los códigos de barras es suficientemente compatible con los equipos electrónicos que los lee.
c) Prueba de lavado: determinar la durabilidad cuando se exponen a condiciones simulando —accidental‖ lavado a máquina.
d) Pruebas de exposición ambiental: determinar la susceptibilidad al compromiso cuando se exponen a luz intensa, calor, humedad, agua y vapor.
e) Pruebas de exposición química: determinar la susceptibilidad al compromiso cuando se exponen a comúnmente disponibles productos químicos y gases químicos.
f) Pruebas electrostáticas/magnéticas: determinar la susceptibilidad al compromiso después de la carga eléctrica o exposición a fuentes magnéticas.
g) Pruebas de elevación mecánica: determinar la susceptibilidad de la capa de seguridad comprometerse levantándola y reemplazarlo en el tiquete.
h) Prueba de laminación: determinar la susceptibilidad al compromiso separando la cartulina.
i) Prueba ULTRAVIOLETA: evaluar las características de seguridad ULTRAVIOLETA que pueden o no pueden estar presente en el billete.
j) Alteración pruebas: determinar la susceptibilidad a comprometer por intentos de alteración como corte y la pasta, alteraciones, reproducción del color copia y falsificación de computadora de mano.
k) Los exámenes transparencia: Determinar la susceptibilidad al compromiso cuando se expone a la luz alterna fuentes, microscopios, equipo de amplificación y computadoras.

Estas pruebas se deberán realizar para cada una de las emisiones como parte del procedimiento de aprobación del operador.

Códigos de Barras: para el caso de la impresión de estos códigos como parte de los parámetros de identificación del tiquete, estos deberán cumplir con los requisitos mínimos definidos en la norma ANSI, su equivalente o su actualización en un futuro

1.4. REQUISITOS GENERALES DE LA TERMINAL DE VENTA - TDV

La operación de las terminales de venta estará a cargo de los establecimientos bajo unos lineamientos definidos por el Operador. Deberán tener la funcionalidad necesaria para la captura del número del tiquete de forma que este pueda ser activado, así como del número oculto destapado al rasparse para la validación del premio cuando el tiquete sea ganador. Eventos que deben ser transmitidos al SCJ. La red de comunicaciones para la conexión al SCJ

debe estar localizada en un sitio seguro, al cual solamente permita el acceso a personal autorizado.

Los proveedores del servicio de conectividad ya sea del Operador o un tercero, deberán permitir la realización de pruebas de conexión entre las terminales de venta y el SCJ, para lo cual deberá poner a su disposición de todas las herramientas de hardware y software, los entornos y el personal necesario para la correcta realización de dichas pruebas.

El software de administración y configuración de la red de comunicaciones no debe permitir acceso a usuarios no registrados por el SCJ (se refiere a los estándares ISO 17799 y 27001).

Las terminales de venta ubicadas en los establecimientos para activar los tiquetes deben cumplir mínimo con las siguientes condiciones:

- Estar asegurada en un área protegida de acceso restringido.
- Las terminales de venta deben presentar un diseño que impida el libre acceso al interior del equipo. Es de anotar que aunque las terminales de venta no requieren ser de uso exclusivo para esta actividad, deberán cumplir todos los protocolos de seguridad que garanticen la independencia de este juego de las demás actividades.
- Las terminales de venta deberán tener un punto de tierra correctamente identificado, al cual se conectarán todos los elementos que requieran de electricidad para su funcionamiento (Referirse al RETIE).
- Los cables que suministran la energía y los cables de datos que entran y salen de la terminal no deben ser accesibles al público en general y no podrán ser fácilmente removidos.
- Los puertos de comunicaciones de las terminales deben estar etiquetados e identificados adecuadamente de acuerdo a su función y deben estar dentro de un área restringida para impedir acceso sin autorización al mismo o a sus cables de conexión.
- Todo dispositivo de almacenamiento de datos y programas, incluyéndose los ROM, EPROM, FLASH ROM, DVD, CD-ROM, Compact Flash, y cualquier otro tipo de dispositivo de almacenamiento de datos y programas deberán estar claramente marcados con información suficiente para identificar el software y el nivel de revisión de la información almacenada en los dispositivos.

1.4.1. Requisitos de Identificación física de las terminales de venta

Las terminales deberán tener una identificación única que no sea removible sin dejar evidencia de alteración, las mismas que deberán encontrarse fijas a ella. Dichas placas deberán incluir como mínimo la siguiente información:

- Nombre fabricante o marca.
- Modelo
- Serial asignado por el fabricante

1.5. REQUISITOS GENERALES PARA LA COMUNICACIÓN

Este capítulo se refiere a las comunicaciones entre el Sistema Central del Juego y las Terminales de Venta

1.5.1. Requisitos para los protocolos de comunicación

Cada componente de la Plataforma Tecnológica debe funcionar como indica el protocolo de comunicación implementado por el Operador. El protocolo seleccionado debe utilizar técnicas de comunicación que cuenten con una apropiada detección de errores y/o mecanismos de recuperación, diseñados para prevenir intentos no autorizados de acceso o modificación. Se recomienda el método de encriptación asincrónica, que impida accesos no autorizados y la interceptación o alternación de los datos intercambiados.

La red de comunicaciones deberá soportar los principales protocolos de comunicación existentes en el mercado para la conexión de las terminales de ventas, siempre y cuando cumplan con los requerimientos de conectividad y seguridad (se refiere a los estándares IEEE 802 y 27001). Y deben asegurar como mínimo lo siguiente:

- Todas las comunicaciones críticas de datos deberán fundamentarse en un protocolo e incorporar un plan de detección de error y corrección para asegurar una precisión del 100% sobre los mensajes recibidos.
- Todas las comunicaciones críticas de datos deberán emplear encriptación. El algoritmo de encriptación debe emplear claves variables o una metodología similar para preservar la seguridad de las comunicaciones.
- La comunicación realizada dentro del sistema, en su totalidad debe funcionar de acuerdo a lo indicado por el protocolo de comunicación implementado.

1.5.2. Pérdida de comunicación.

Para el Sistema Central del Juego, una terminal de venta debe ser considerada como no disponible si existe alguna falla de comunicación con el servidor. Por lo tanto, para que un tiquete sea legítimo este debe haber sido validado en línea con el SCJ, la transacción reportada y registrada tanto en el SCJ como con el administrador del juego, mediante un sistema de transmisión directa y en línea del proceso de validación. Es de aclarar, que el Operador podrá permitir validar un paquete de tiquetes previos a su venta, pero esta es una estrategia comercial, para el SCJ todos los tiquetes se consideran vendidos al momento de validarlos independiente de la entrega física al cliente, por lo tanto el Operador responderá por la venta de estos tiquetes para efectos de derechos de explotación al momento de su validación.

La validación del premio solo es posible mediante una consulta en línea con el SCJ, por lo tanto quedará suspendida hasta que se reactive la comunicación con ese Punto de Venta, aunque el poseedor del tiquete podrá de igual cobrarlo en cualquier otro Punto de Venta que posea comunicación con el SCJ.

2. REQUISITOS TECNOLÓGICOS DEL SISTEMA CENTRAL DEL JUEGO – SCJ.

2.1. BATERIA DE RESERVA

El servidor o los servidores del SCJ, deberán retener la información requerida después de una pérdida de energía eléctrica por un plazo de tiempo determinado, que inicialmente se ha definido de noventa y seis (96) horas. Si estos datos son almacenados en la memoria de acceso aleatoria RAM volátil, deberá instalarse una batería de respaldo para el o los servidores.

2.2. RELOJ DEL SISTEMA

El reloj del sistema debe reflejar la hora actual en formato local de fecha y hora, el SCJ debe ser compatible con el reloj del sistema operativo y se deberá sincronizar los relojes de los Servidores y las Terminales de Ventas. Como referencia de la hora oficial, se tendrá en cuenta la suministrada por la Superintendencia de Industria y Comercio.

2.3. BASE DE DATOS DEL SISTEMA CENTRAL DEL JUEGO

Los servidores del Sistema Central del Juego, deberán contener una base de datos, en donde quedará almacenada en línea y en tiempo real el detalle de la información de control y las transacciones generadas por las terminales de ventas. Para el repositorio de los datos, se deberá contar con un sistema manejador de base de datos, capaz de realizar automáticamente planes de mantenimiento y *backups*, *logs* de las transacciones, control de acceso a las tablas y niveles de privilegios. La base de datos deberá tener los respaldos necesarios para garantizar su correcto funcionamiento.

2.3.1. Acceso a la base de datos

El SCJ contará con mecanismos de verificación y control, que permitan la auditoria continua del sistema, evitando la modificación directa o indirecta de la base de datos. Todo el personal autorizado (usuarios) a operar el SCJ mantendrá un control permanente de acceso seguro al sistema. El administrador del juego deberá disponer de acceso local y remoto de solo lectura a la base de datos, que permita acceder a la información de control correspondiente a las apuestas y registros de auditoría (se refiere a los estándares ISO 17799 y 27001).

2.3.2. Información almacenada en la base de datos

El SCJ en el servidor o servidores almacenará una base de datos que como mínimo debe contener:

Información Administrativa. Se refiere a la información correspondiente al Operador del SCJ y a la información de identificación de la terminal de ventas. Esta información deberá estar

almacenada en una o más bases de datos del Operador de donde se extraerá cuando sea solicitada por el administrador del juego y/o el interventor. Deberá incluir como mínimo

a) Información del Operador:

- Nit del Operador.
- Permiso otorgado por el administrador del juego.
- Numero de contrato otorgado por el administrador del juego.
- Fecha de inicio del contrato.
- Fecha final del contrato.

b) Información del establecimiento:

- Código del establecimiento o punto de venta.
- Nombre.
- Dirección.
- Municipio (Código DANE)

c) Información de la Terminal de Punto de Venta (TPV):

- Identificación única de la Terminal.
- Nombre fabricante o marca.
- Serial
- Modelo.

Información de Control. Se refiere a los eventos significativos que se generan desde una terminal de venta y se envían al SCJ. Cada evento deberá ser almacenado en una o más bases de datos del Operador de donde se extraerá cuando sea solicitada por el administrador del juego y/o el Interventor. Debe incluir como mínimo la siguiente información:

- La fecha y hora en que ocurrió la incidencia.
- La identidad de la terminal de punto de venta que generó la incidencia.
- Un número/código exclusivo que defina la incidencia.
- Un texto breve que describa la incidencia.
- Cualquier otra información que se acuerde con el administrador del juego.

Información de Transacciones. Se refiere a los tiquetes vendidos y premios pagados desde una terminal de venta y que se envían al SCJ. Cada evento deberá ser almacenado en una o más bases de datos del Operador de donde se extraerá cuando sea solicitada por el administrador del juego. La información de los tiquetes en el SCJ, deberán permitir su identificación. La siguiente es la información de las transacciones que deberán ser transmitidas por la terminal de venta al SCJ, en pesos colombianos:

- Tiquetes validados (Entradas): Acumula el valor total de todos los tiquetes validados que para efectos del juego, equivalen a estar vendidos. El SCJ mantendrá la información proporcionada por las terminales de venta, de los tiquetes activados

- Tiquetes ganadores (Salidas): Acumula el valor total de todos los montos pagados por los tiquetes premiados.
- Retorno de la Emisión: Acumula el valor de los montos pagados por tiquetes ganadores menos montos pagados por tiquetes
- Anulaciones
- Tiquetes jugados: El SCJ debe tener contadores que acumulen el número de tiquetes emitidos, validados, premiados y anulados por terminal de venta, de forma que se permita hacer un análisis detallado de los resultados de la Emisión.

Información de auditoría. Se refiere a los registros de los eventos de auditoría propios del SCJ, cada evento deberá ser almacenado en una o más bases de datos del Operador, y serán los registros sobre los cuales el administrador del juego y/o el interventor designado realizará las auditorias. Deberán incluir como mínimo los siguientes datos:

- Fecha y hora en que aconteció el suceso.
- Operador.
- Establecimiento de juego
- Identificación terminal de ventas.
- El o los números del suceso(s) significativo(s).
- La fecha y hora en que aconteció el suceso.
- Un texto breve que describa el suceso en el idioma español.

Información de auditoría de escrutinio: Se refiere a los registros de los eventos de auditoría propios del SCJ, que se podrían realizar en cualquier momento de vigencia de la emisión, pero que sobre todo se realizarán al finalizar la emisión, para permitir el análisis de dicha emisión en aspectos concernientes a ventas por punto de venta, resultados económicos, etc.

Como mínimo se deben tener en cuenta los siguientes eventos de auditoría:

- Registros en una tabla de la base de datos de la fecha, hora y tramas transmitidas hacia el administrador del juego.
- Registros de cualquier intento de modificación o alteración de la información en la base de datos.
- Registros de las operaciones realizadas en las bases de datos, para lo cual se requerirá de un motor de bases de datos que permita realizar dicha operación automáticamente.

2.4. ESTACIONES DE TRABAJO DEL SCJ

El SCJ contará con una terminal o estación de trabajo que facilite a las personas autorizadas (usuarios) el acceso al sistema en el cual se deben encontrar definidos diferentes niveles de acceso para cada usuario.

El SCJ contará a su vez, con una estación de trabajo que permita el acceso al aplicativo desde el cual se realizan las labores de auditoría y seguridad en la información registrada en la base

de datos. El *software* de administración y configuración del SCJ, no debe permitir acceso a usuarios no registrados (se refiere a los estándares ISO 17799 y 27001).

3. REQUISITOS DE SEGURIDAD

El Operador debe garantizar las condiciones de seguridad física y lógica de toda la plataforma tecnológica que soporta el sistema de lotería de instantánea, de forma que se asegure la integridad del sorteo y de la información almacenada. Como mínimo el centro de cómputo principal donde esté ubicado el Sistema Central del Juego deberá ser nivel TIER III (Centro de datos concurrentemente mantenible: disponibilidad garantizada de 99.982 %).

Debe existir un centro de cómputo alterno, que garantice la operación del juego, ubicado en un área geográfica diferente al centro de cómputo principal. El centro de cómputo alterno debe estar en capacidad de continuar la actividad del juego en un plazo máximo de 24 horas, en caso de falla del centro de cómputo principal. Se debe tener cuenta que durante el plazo que el SCJ no este activo, no podrá generarse ninguna transacción (venta de tiquetes y pago de premios).

La transmisión de información entre el Sistema Central del Juego y los diferentes terminales de venta, será a través de una red de comunicaciones confiable y segura, preferiblemente redundante, protegida contra amenazas internas y externas a través de tecnologías protectoras, y con algún sistema de encriptación asincrónico. El Operador presentará al administrador del juego la topología de su red para su aprobación.

El Operador deberá contar con un DRP (*Disaster Recovery Plan*) aprobado por el administrador del juego, cuyos protocolos deberán ser seguidos en caso de falla total de la Plataforma Tecnológica y por lo tanto del Sistema Central del Juego, con el objetivo de recuperar el sistema mediante los planes de contingencia establecidos. La recuperación de la data deberá estar garantizada en un término no mayor a 24 horas después de ocurrida la contingencia.

La plataforma tecnológica que soporta el sistema deberá cumplir mínimo con los siguientes requisitos de seguridad (se refiere al estándar de ISO 27001):

- La transmisión de la información se deberá realizar mediante algoritmo de cifrado asimétrico, garantizando la privacidad de los datos que son transportados dentro de la red.
- Deberá contener un módulo de auditoría.
- Se debe garantizar la efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad de la información que fluye entre el SCJ y las terminales de venta.
- La información de los eventos: de control, de tiquetes validados (vendidos) y premiados (pagados) almacenada en el SCJ debe conservarse en las bases de datos o en respaldos históricos mínimo seis (6) años.
- Cumplir como mínimo con el estándar de seguridad "C2" del NCSC (*National Computer Security Center*), el cual contiene las políticas de seguridad de acceso para los sistemas operacionales.

- El SCJ no permitirá modificar la información que se obtenga desde la terminal de venta, y deberá notificar al administrador del sistema y bloquear al usuario tras un número fijo de intentos de ingreso frustrados.
- El SCJ deberá ser diseñado para proteger la integridad de los datos importantes en la eventualidad de una falla.
- Los registros de auditoría, base de datos del sistema y cualquier otro dato importante debe ser almacenado utilizando métodos de protección razonables.
- Cumplir con condiciones de seguridad tanto física como lógica que impidan accesos no autorizados al *software* y bases de datos.
- Proteger las claves de acceso a los sistemas de información, bases de datos y sistemas operativos. En desarrollo de esta obligación, los Operadores deberán evitar el uso de claves compartidas, genéricas o para grupos. La identificación y autenticación en los dispositivos y sistemas de cómputo de los establecimientos autorizados deberá ser única y personalizada.
- Si se utilizan discos duros como medio de almacenamiento, se debe asegurar la integridad de los datos en el evento de una falla del disco. Los métodos aceptables incluirán, pero no estarán limitados a, múltiples discos duros en una configuración aceptable RAID, o replica/duplicado de datos entre dos o más discos duros, el método utilizado deberá proporcionar también un soporte abierto para copias de seguridad y restablecimiento.
- La implementación del esquema de copia de seguridad deberá ocurrir al menos una vez todos los días.
- Manejo y seguridad de los medios de almacenamiento.
- Requisitos para la Recuperación. En el evento de una falla catastrófica, cuando el SCJ no pueda ser reiniciado de ninguna otra forma, deberá ser posible volver a cargar la base de datos desde el último punto de copia de seguridad viable y recuperar totalmente los contenidos de esa copia de seguridad; se recomienda que consista de al menos la siguiente información:
    - Eventos significativos.
    - Información de auditoría.
    - Información del sitio especifico como la configuración de la terminal, cuentas de seguridad, etc.
- Contar con un sistema de certificación de origen de datos que garantice que el emisor de la información solicitada por el administrador del juego es válido y autorizado para enviar información.

3.1 ACCESO A LA CONFIGURACIÓN DEL JUEGO

El software de administración y configuración del SCJ, no debe permitir acceso a usuarios no registrados (se refiere a los estándares ISO 17799 y 27001).

Protección Contra Intrusiones. Todos los servidores tendrán la suficiente protección física/lógica contra accesos no autorizados. Idealmente, el sistema requerirá proveer el acceso en conjunto pero no separados del administrador del juego y el Operador.

Requisitos del Acceso a la Configuración. El menú de configuración/instalación del SCJ no debe estar disponible por personal no autorizado y debe utilizar un método de acceso.

Programación del Servidor. No habrá medios disponibles para que un Operador lleve a cabo una programación en el servidor que permita modificar la base de datos de resultados de los eventos y las transacciones generadas en las Terminales de Venta.

Protección contra Virus. Es recomendable que todos los servidores, terminales y dispositivos del SCJ deben contar con una protección contra virus adecuada.

Protección contra Copias. Una protección contra copias, para prevenir la proliferación no autorizada o modificación del software, para servidores o terminales, puede ser implementada siempre y cuando que:

- El método de protección contra copias este totalmente documentado; y
- Cualquier dispositivo envuelto en hacer cumplir la protección contra copias podrá ser verificado individualmente.

3.2 CONTROL DE ACCESO

El SCJ deberá contar o con una estructura jerárquica de personificación por la cual el nombre del usuario y la contraseña definen el acceso a los programas y a las opciones, en particular de menús, o bien admitirá el acceso a programas y dispositivos de forma segura, basándose estrictamente en el nombre del usuario y contraseña. Se puede fortalecer la seguridad del acceso remoto, por medio de un elemento de soporte físico (*hardware*) y una firma digital que autentique y garantice el acceso autorizado. El SCJ, no permitirá ninguna alteración del registro de información significativa que haya sido comunicada desde la terminal de venta. Adicionalmente, deberá existir la funcionalidad para notificar al administrador o generar el registro de auditoría correspondiente, cuando ocurra un número determinado de intentos de entradas de acceso fracasadas y bloqueo de usuario.

Deberá cumplir mínimo con las siguientes condiciones:

- El Operador deberá establecer un protocolo de acceso físico y lógico a sus sistemas técnicos del juego en el que se recojan los procedimientos para su control, la relación de las personas que dispongan de autorización para el acceso, así como las operaciones que pueden realizar en los sistemas.
- El registro de acceso al Sistema Central del Juego y su réplica, deberá ser conservado por el Operador durante, al menos, dos (2) años.
- El Sistema Central del Juego y su réplica serán accesibles únicamente por las personas expresamente designadas por el Operador a estos efectos y, en el marco de una inspección, por el administrador del juego y/o el interventor.
- El Operador deberá establecer las medidas de seguridad físicas y lógicas que aseguren el control del acceso a los sistemas técnicos, que impidan el acceso y permitan la detección de cualquier persona no autorizada.

- El Operador deberá realizar mínimo una vez al año pruebas de vulnerabilidad a los diferentes sistemas y plataformas de información utilizada para la operación del juego.
- Seguridad en la definición de cargos del personal.
- Protección contra software malicioso y virus informáticos.
- Gestión, control y seguimiento del acceso a usuario del sistema.
- Control y seguimiento de acceso a redes, sistema operativo y aplicaciones.
- Seguridad en el desarrollo y mantenimiento de los sistemas.

3.3 SEGURIDAD EN EL SISTEMA DE COMUNICACIÓN

Todas las comunicaciones al Sistema Central del Juego, incluido el Acceso Remoto, deben pasar a través de por lo menos un cortafuego (*firewall*) a nivel aplicación (*application-level*) aprobado y no tendrá la facilidad de permitir una ruta de red alterna. Si existe una ruta de red alterna para propósitos de redundancia, esta también debe pasar a través de por lo menos un cortafuego (*firewall*) a nivel aplicación (*application-level*).

Esta aplicación de Cortafuegos (*firewall*) debe mantener un registro de auditoría de la siguiente información y debe desactivar todas las comunicaciones y generar un evento de error si el registro de auditoría se llena en su totalidad:

- Todos los cambios de configuración del cortafuego (*firewall*);
- Todos los intentos de conexión exitosos o fallidos* hechos a través del cortafuego (*firewall*); y
- Direcciones IP de la fuente y destino, Número de Puerto y Direcciones MAC.

3.4 SEGURIDAD EN EL ACCESO REMOTO

El acceso remoto es definido como cualquier acceso al SCJ desde afuera del sistema de red confiable. Para el acceso al SCJ en forma remota deberá cumplir con las mínimas condiciones de seguridad exigidas, como lo son el uso de *firewall* lógicos o físicos, VPN, usuario y contraseña (se refiere a los estándares ISO 27001). Para el caso de acceso remoto seguro por internet, este debe ser seguro, fiable y apropiado a sus aplicaciones, utilizando para ello la encriptación SSL estándar y la tecnología de navegación web para solucionar los problemas de acceso, sin tener requisitos de entorno del usuario. De los accesos al SCJ se debe registrar la información que permita posteriormente realizar un seguimiento de un evento ocurrido. El acceso remoto debe cumplir con siguientes requisitos:

- Generar el registro de la actividad de los usuarios por acceso remoto, que describa el nombre del usuario, la fecha y hora, duración y la actividad desarrollada durante el acceso.
- No se permitirá funcionalidades administrativas por usuarios remotos sin autorización (por ejemplo, agregando usuarios, cambiando permisos, etc.)
- No se permitirá el acceso a la base de datos sin autorización.
- No se permitirá el acceso al sistema operativo sin autorización.

- Si la base de datos del acceso remoto es constante, se deberá instalar un filtro de red (*firewall*) o un sistema diseñado para prevenir el acceso de usuarios no autorizados y proteger la información de ataques externos.

Auditoría de Acceso Remoto. El sistema central debe mantener un registro de actividad ya sea automáticamente, o permitiendo el ingreso manual de dicho registro describiendo toda información de acceso remoto que incluya:

- Nombre de acceso;
- Tiempo y fecha de cuando la conexión fue realizada;
- Duración de la conexión; y
- Actividad mientras esta registrado, incluyendo el acceso a áreas específicas y cambios que fueron realizados.

El SCJ debe tener la funcionalidad para el acceso remoto con el propósito de permitirle al administrador del juego el acceso a los datos necesarios y especificados en este documento. El acceso a los datos almacenados en el SCJ podrá ser por medio de productos de un tercero siempre y cuando el acceso sea seguro.

NOTA: Se reconoce que el fabricante del SCJ podrá acceder de forma remota al Sistema y a sus componentes asociados con el propósito de soportar la solución. Sin embargo, este acceso deberá ser autorizado y por un medio seguro.

3.5 ALTERACIÓN DE DATOS

El SCJ no permitirá la alteración de la información de control, ni de transacciones transmitidos desde las TPV. Si por alguna razón se modifica esta información, se debe generar un registro automático de auditoría con la siguiente información:

- El dato alterado.
- El valor del dato previo a la alteración.
- El valor del dato después de la alteración.
- La hora y fecha de la alteración.
- El usuario que realizó la alteración (usuario activo en el SCJ).

3.6 LAS COPIAS DE RESPALDO Y RECUPERACIÓN

Habrá copias redundantes de cada archivo de registro o base de datos del sistema o ambos en el SCJ con soporte abierto para las copias de seguridad y recuperación (se refiere al estándar ISO 27001).

3.7 REQUISITOS PARA LA RECUPERACIÓN

En caso de un fallo del SCJ, el sistema deberá tener la capacidad de recargarse desde las copias de seguridad, recuperando plenamente los contenidos en un plazo no mayor a 12 horas. Se recomienda que se incluya como mínimo la siguiente información:

- Información de auditoría.
- Información administrativa.
- Información de control.
- Contadores.

El SCJ no permitirá la modificación o alteración de ninguna información de control o contadores que haya sido comunicado desde la terminal de venta, conservando la trazabilidad de cualquier intento de modificación o alteración en los registros del SCJ (Se refiere al estándar ISO 27001).

3.8 REGISTRO, TRAZABILIDAD DE LAS OPERACIONES DE JUEGO Y LA BASE DE DATOS.

- El Sistema Central del Juego debe garantizar la trazabilidad y el registro de la totalidad de las operaciones de juego que se realicen, permitiendo la reconstrucción fiel de las transacciones realizadas: tiquetes validados, tiquetes premiados-pagados y tiquetes cancelados.
- El Sistema Central del Juego realizará la captura, registro y conservación de las transacciones.
- Todos los elementos del Sistema Central del Juego deberán estar protegidos física y lógicamente e impedir cualquier acceso no autorizado.
- Los Operadores también incluirán en la Base de Datos segura:
  - Los datos de control mínimos establecidos por el administrador del juego.
  - Un registro de incidencias que incluya al menos las interrupciones del servicio de validación de tiquetes y pago de premios.
  - Cualesquiera otros datos requeridos por el administrador del juego de forma general o individual en un procedimiento de control.
- La base de datos segura y los registros del Operador deberán conservarse por un período mínimo de seis (6) años, debiéndose establecer los sistemas de protección y respaldo que aseguren su integridad y seguridad durante ese plazo, así como su recuperación íntegra ante eventualidades.

3.9 CONTINUIDAD DE LA ACTIVIDAD DE JUEGO

- El Plan de Contingencia Tecnológica contemplará las medidas técnicas, humanas y organizativas necesarias para garantizar la continuidad del servicio dentro de un plazo no mayor de 24 horas. El Operador deberá informar adecuadamente sobre sus políticas en relación con las interrupciones del servicio y la forma en que los clientes pueden verse afectados. El Operador adoptará las medidas necesarias para garantizar que sus clientes reciban un trato justo en caso de interrupción la venta de tiquetes o pago de premios.
- El Plan de Contingencia Tecnológica deberá garantizar que, en ningún caso, se pierdan datos o transacciones que afecten o puedan llegar a afectar al desarrollo de la lotería, a los derechos de los participantes o al interés público.

- El administrador del juego evaluará el plan de contingencia tecnológica del Operador y, en su caso, requerirá al Operador la adopción de las medidas adicionales que considere precisas para asegurar la continuidad de las actividades del juego.
- El Operador realizará por lo menos un simulacro al año del plan de contingencia tecnológica para lo cual deberá invitar a Coljuegos y/o al interventor.

4. ASPECTOS ADMINISTRATIVOS

Asegurar la puesta en funcionamiento de la totalidad del Sistema del Juego de Lotería Instantánea y soporte requeridos, para lo cual es necesario que se tengan implementados por lo menos los siguientes procesos, los cuales corresponden a las mejores prácticas de administración de sistemas (se refiere al estándar ISO 9001):

- Administración de niveles y continuidad del servicio
- Administración de los servicios de terceros
- Administración del desempeño y capacidad
- Administración de la seguridad de los sistemas
- Educación y entrenamiento a los usuarios
- Administración de la configuración
- Administración de los problemas
- Administración de los datos
- Administración del ambiente físico
- Administración de las operaciones
- Procedimientos a seguir cuando se evidencia alteración o manipulación de las máquinas o información.

5. CERTIFICACIÓN

El Operador seleccionado deberá someter su Sistema Central del Juego ante un laboratorio certificador autorizado por el administrador del juego, para que realice las pruebas necesarias y le otorgue una certificación en idioma español, de su cumplimiento de los Requerimientos Técnicos indicados en el presente documento. Los costos de esta certificación estarán a cargo del operador y los resultados deberán ser dirigidos directamente al administrador del juego.

Dicho laboratorio realizará ensayos de seguridad, cumplimiento y funcionalidad, basados en los requisitos indicados en este documento y cualesquiera otros requisitos técnicos desarrollados de acuerdo con las funcionalidades y especificaciones del producto del Operador adjudicado, con la finalidad de garantizar la integridad y transparencia de la operación de los equipos y software que son parte de la solución tecnológica.

Los ensayos al Sistema Central del Juego deberán ser realizados, ya sea en las instalaciones del laboratorio o en las instalaciones del proveedor del sistema, en donde el laboratorio realizará las pruebas al sistema en conjunto con las terminales de juego con el equipo

ensamblado y también en campo donde la instalación y comunicación será probada antes de su implementación.

El operador también será objeto de inspecciones anuales de campo y cualquier otro tipo de procedimientos de auditoría y fiscalización que el administrador del juego requiera realizar para garantizar la transparencia e integridad.

Cualquier adición de juegos, modificación u actualización de los ya existentes que implique cualquier cambio en el sistema original, deberá ser sometido a un proceso de control de calidad y aprobación en conjunto entre el Operador y administrador del juego previo a su puesta en producción.

El costo de los procesos de certificación y fiscalización en campo debe ser asumido por el Operador las veces que sea requerido.