SERIES DE ESTÁNDARES TÉCNICOS

GLI-13:

Sistemas Monitoreos y de Control En Línea (SMC) y Sistemas de Validación en Casinos

Versión: 2.1

Fecha de Publicación: 6 de Septiembre del 2011

SOBRE ESTE ESTÁNDAR

Este estándar ha sido producido por **Gaming Laboratories International, LLC** con el propósito de proporcionar certificaciones independientes a los fabricantes bajo este Estándar y cumplir con los requisitos establecidos en este documento.

Un fabricante debe presentar equipo con una petición que sea certificado de acuerdo con este Estándar. A partir de la certificación, Gaming Laboratories International, LLC., suministrará un certificado evidenciando la certificación a este Estándar.

Sistemas Monitoreos y de Control En Línea

GLI-13 Revisión 2.1

Publicación: 6 de Septiembre del 2011 V2.1 Final
Publicación: 20 de Abril del 2007 V2.0 Final
Publicación: 30 de Junio del 2006 V1.2 Borrador para Comentarios
Producido: 20 Febrero 2001 V1.1

Historial de Revisiones

Para el historial de revisiones de este estándar, comuníquese con nuestra oficina.

Tabla de Contenido

CAPITULO 1

1.0 VISIÓN GENERAL – ESTÁNDAR PARA SISTEMAS MONITOREO Y DE CONTROL

1.1 Introducción

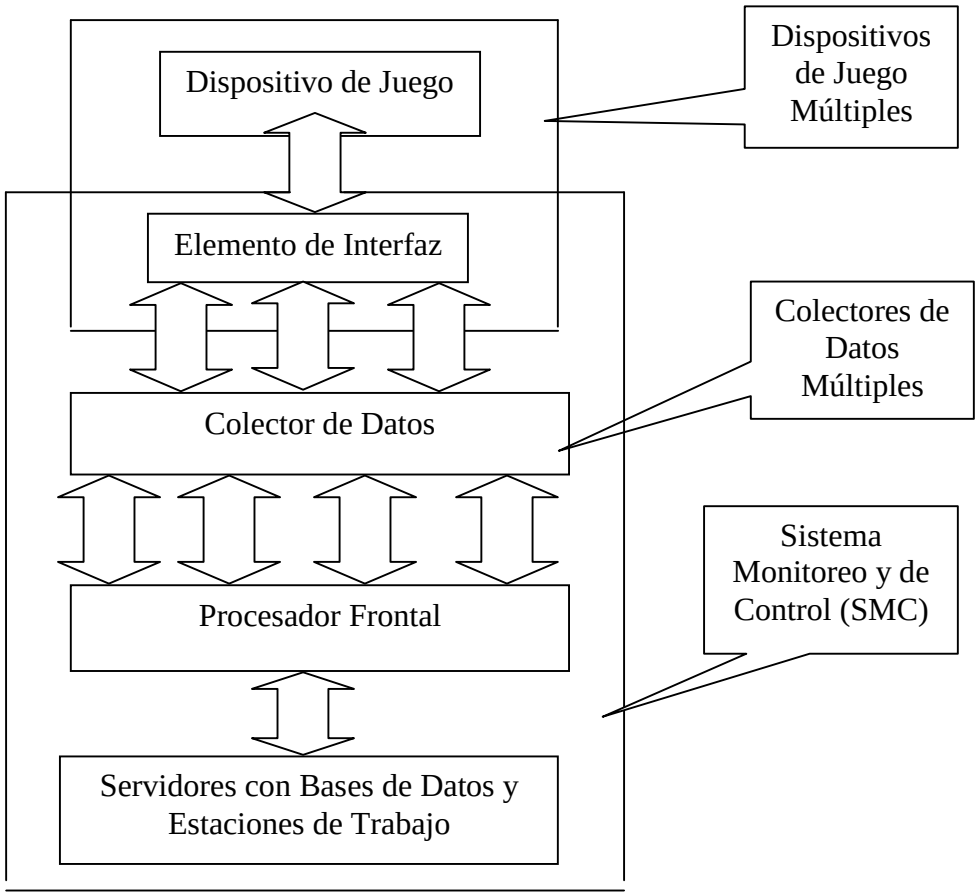
1.1.1 Definición de un Sistema Monitoreo y de Control en Línea. Un Sistema Monitoreo y de Control en Línea ("SMC") es un sistema de administración de juego que continuamente monitorea cada dispositivo de juego electrónico por medio de un protocolo de comunicación especifico ya sea por una línea dedicada, sistema de conexión por línea conmutada u otro método de transmisión asegurada. La tarea principal de un "SMC" es de proporcionar registros de datos, búsquedas e informes de los eventos significativos de juegos, colección de datos financieros de los dispositivos individuales y datos de contadores, reconciliación de los datos de contadores contra los conteos electrónicos y actuales y la seguridad del sistema detallado en la sección 4.0 de este documento.

1.1.2 Fases de la Certificación. La aprobación de un Sistema Monitoreo y de Control en Línea será certificada en dos fases.

a) Los ensayos iniciales en el laboratorio, donde el laboratorio ensayará la integridad del sistema en conjunto con los dispositivos de juego, en un ambiente de laboratorio con el equipo ensamblado; y
b) Certificación in situ donde las comunicaciones y configuraciones son ensayadas en la localidad del casino, previamente a la implementación.

1.2 Visión General Gráfica

1.2.1 Declaración General El propósito de esta sección es de prestar una ilustración visual de un sistema computarizado tipo Monitoreo y de Control genérico, pero no es pretendido para obligar ningún componente en particular o topología estipulando que la funcionalidad debe ser mantenida. Los términos utilizados en este documento serán representados en un formato de diagrama de bloques para aclarar cada componente individual.



En la ilustración anterior, este estándar aplica a todos los componentes referenciados no incluyendo los dispositivos de juego. Los requisitos para el dispositivo de juego están definidos en GLI-11. Este documento sólo se concentra en las comunicaciones desde el dispositivo de juego al "SMC", y no en el orden inverso con la excepción de los requisitos de Sistema de Validación de boletos/vales incorporados en el capítulo 4.
.

1.3 Reconocimiento de otros Estándares Evaluados

1.3.1 Declaración General. Estos estándares han sido desarrollados por medio de evaluaciones y utilizando porciones de los documentos de las organizaciones listadas a continuación. Nosotros reconocemos los reguladores que han ensamblado estos documentos y los agradecemos:

a) La Oficina de Administración Financiera ACT;
b) El Departamento de Juegos y Carreras de Nueva Gales del Sur;
c) La Autoridad de Control de Casinos de Nueva Zelandia;
d) El Departamento de Asuntos Internos, Juegos de Carreras y División de Censura de Nueva Zelandia;
e) La Autoridad de Carreras y Juegos del Territorio Norteño;
f) La Oficina de Regulaciones de Juegos de Queensland Australia;
g) La Oficina de Sur Australia de Bebidas Alcohólicas y Comisión de Juegos;
h) El Departamento de Tesorería y Finanzas, Ingresos y División de Juegos de Tasmania;
i) La Autoridad de Casinos y Juegos de Victoria Australia;
j) La Oficina de Juegos de Carreras y Bebidas Alcohólicas de Australia Occidental.
k) Los SABS, 1718 parte 3;
l) Pactos Tribales de los Estados Unidos de los Gobiernos Tribales y los Gobiernos Estatales incluyendo:
   i. Arizona
   ii. Connecticut
   iii. Iowa Indios
   iv. Kansas
   v. Louisiana
   vi. Michigan
   vii. Minnesota
   viii. Mississippi
   ix. North Carolina
   x. North Dakota
   xi. Oregon
   xii. Wisconsin
m) División de Juego – Regulaciones de Juegos Limitados del Estado de Colorado;
n) Las Regulaciones Adoptadas por el Comité de Juegos del Estado de Illinois;
o) La Comisión de Juego del Estado del Estado de Indiana;
p) La Comisión de Juego y Carreras del Estado de Iowa;
q) Policía del Estado de Louisiana – División de Juego – Dispositivos de Juego;
r) Comisión de Juego del Estado de Missouri – Departamento de Protección Civil;
s) Comisión de Juego del Estado de Nevada y el Comité de Control de Juego del Estado
t) Regulaciones de Contabilidad y Controles Internos del Estado de New Jersey
u) Las Reglas y Regulaciones para los Juegos Limitados de la Comisión de Juegos de Estado de South Dakota.
v) Publicación Especial NIST, 800-57, Recomendaciones para la Administración Clave – Parte 2: Mejores Prácticas para la Organización Administrativa Clave
w) Estándar Regulatorio Técnico 14 del Estado de Nevada;
x) Los Estándares de Protocolos GSA, G2S and S2S; y
y) Los Estándares Técnicos GLI-11, GLI-13, and GLI-20

1.4 Propósito del Estándar

1.4.1 Declaración General. El propósito de este estándar técnico es lo siguiente:

a) Eliminar criterio subjetivo en el análisis y certificación operacional de Sistemas Monitoreo y de Control de Juego.

b) Solamente ensayar los criterios que impactan la credibilidad y la integridad de juego por ambas partes del punto de vista de la colección de ingresos y del juego.

c) Crear un estándar que asegurará que los Sistemas Monitoreo y de Control En Línea ("SMC") y los sistemas de validaciones en Casinos son honrados, seguros, y que puedan ser auditables y operados correctamente.

d) Para distinguir entre la política pública local y el criterio del Laboratorio. En GLI, nosotros creemos que es la responsabilidad de cada jurisdicción local de fijar su propia política pública con respecto al juego.

e) Reconocer que los ensayos que no son relacionados al juego (como ensayos de electricidad) no deben ser incorporados dentro de este estándar, pero dejados a las pruebas apropiadas de los Laboratorios que especializan en estos tipos de pruebas. Exceptuando donde se identifica específicamente en el estándar, pruebas no son dirigidas a los asuntos de salud o protección. Estos asuntos son la responsabilidad del fabricante, comprador y operador del equipo.

f) Construir un estándar que pueda ser cambiado o modificado fácilmente para permitir tecnología nueva.

g) Construir un estándar que no especifique ninguna tecnología en particular, método o algoritmo. La intención es de permitir un rango ancho de métodos para ser utilizados en conforme a los estándares mientras que al mismo tiempo, dar aliento al desarrollo de nuevos métodos.

1.4.2 Sin Limitación de Tecnología. Uno debe tener precaución que este documento no sea leído de tal manera que limita la utilización de tecnología en el futuro. Este documento no debe ser interpretado de manera que si la tecnología no está mencionada, entonces no es permitida.
Totalmente lo contrario, cuando alguna tecnología nueva es desarrollada, nosotros repasaremos este estándar, realizaremos cambios e incorporaremos nuevos estándares mínimos para la tecnología nueva.

1.4.3 Alcance del Estándar. Este estándar solamente gobernará los requisitos de Sistemas Monitoreo y de Control necesarios para lograr una certificación cuando esté interconectado a dispositivos de juegos, con el propósito de comunicar eventos mandatorios de seguridad y contadores electrónicos. Esto deduce que todas las transacciones monetarias pertinentes al nivel del dispositivo de juego son manejadas a través de:

a) Emisión de Créditos:
   i. Monedas o fichas aceptadas por medio de un aceptador de monedas aprobado;
   ii. Dinero en Efectivo (Billetes) aceptados por medio de un verificador de billetes aprobado; y
   iii. Boleto/Vale Aprobado (Artículos) aceptados por medio de un validador de Billetes/Boletos/Vales; o
   iv. Tarjeta de la Cuenta del Jugador (Sin Dinero en Efectivo)

b) Redención de Créditos:
   i. Monedas o fichas pagadas por tolvas aprobadas;
   ii. Pagos Manuales;
   iii. Boletos/Vales pagados por una impresora de boletos/vales; o
   iv. Tarjetas de la Cuenta del Jugador (Sin dinero en efectivo).

1.4.4 Excepciones al Estándar. Este estándar no gobierna requisitos de un "SMC" para cualquier otra forma de transacción monetaria. Este estándar tampoco no gobierna protocolos de comunicación bidireccionales avanzados (por ejemplo, Transacciones de fondos electrónicos (EFT), Transacciones de fondos avanzados (AFT), Bonificaciones, Promociones, Progresivos basados en Sistema, facciones que utilizan un RNG, etc.) que apoyan transferencias de créditos entre el dispositivo de juego y el "SMC". Este estándar solo apoya la comunicación unidireccional de eventos originando al nivel del dispositivo de juego hacia el "SMC" con excepción de los requisitos del sistema de validación de boletos/vales. Este estándar no excluye los dispositivos de juegos que operan con transacciones sin dinero en efectivo de cuentas de jugadores con el propósito de comunicar eventos de seguridad y los contadores electrónicos mandatorios. Esto deduce que todas las transacciones monetarias relativas al nivel del dispositivo de juego electrónico son manejadas por transferencia electrónica a través de un protocolo de comunicación asegurado. Estos tipos de dispositivos deben cumplir con los requisitos aplicables establecidos en este documento, específicamente gobernando la información de contadores y eventos significativos en adición a otros estándares GLI que puedan aplicar.

1.5 Otros Documentos que Pueden Aplicar

1.5.1 Declaración General. Este estándar cubre los requisitos mínimos de un "SMC" and todo componente asociado. Por favor refiérase al sitio de internet de GLI www.gaminglabs.com para otros estándares GLI. A continuación se presentan algunos que pueden ser aplicables:

a) Dispositivos de Juegos en Casinos (GLI-11);
b) Dispositivos de Juegos Progresivos en Casinos (GLI-12);
c) Sistemas Sin Dinero en Efectivo en Casinos (GLI-16);
d) Sistemas de Bonificación en Casinos (GLI-17);
e) Sistemas Promocionales en Casinos (GLI-18);
f) Procedimientos Mínimos de Control Interno de la Comisión de Juego Individual;
g) Terminales de Redención (GLI-20);
h) Sistemas Cliente/Servidor (GLI-21); y
i) Sistemas de Juegos Inalámbricos (GLI-26).

CAPITULO 2

2.0 REQUISITOS PARA LOS COMPONENTES DEL SISTEMA.

2.1 Requisitos de los Elementos de Interfaz

2.1.1 Declaración General. Cada máquina de juego electrónica instalada en una sala de juego deberá tener un dispositivo o facilidad (es decir, un elemento de interfaz) instalado dentro de la máquina de juego electrónica en un área asegurado, que proporcione la comunicación entre el Dispositivo de Juego y un Colector de Datos externo.

2.1.2 Requisitos para los Contadores. Si no se están comunicando los contadores de los Dispositivos de Juego directamente, el elemento de interfaz deberá mantener contadores electrónicos separados, de longitud suficiente para prevenir la pérdida de información de los contadores cuando rueden a cero (0) o un medio de poder identificar múltiples ruedas a cero (0) según lo dispuesto en los dispositivos de juegos conectados. Estos contadores electrónicos serán capaces de ser mostrados por solicitud, a nivel del elemento de interfaz a través de un método de acceso autorizado, refiérase también a la sección titulada 'Contadores' de este documento.

2.1.3 Requisitos de la Batería de Respaldo. El elemento de interfaz deberá retener la información requerida después de una pérdida de energía eléctrica por un plazo de tiempo determinado por la comisión regulatoria. Si estos datos son almacenados en la memoria de acceso aleatoria RAM volátil, una batería de respaldo debe ser instalada dentro del elemento de interfaz, refiérase también a la sección titulada 'Contadores' de este documento.

2.1.4 El Intermediario de Información. En los casos que la información requerida no pueda ser comunicada al "SMC", el elemento de interfaz debe proporcionar un método para preservar toda la información de los contadores obligatorios y la información de los eventos significantes hasta el momento en cual la pueda comunicar al "SMC", refiérase también a las secciones tituladas 'Eventos Significantes' y 'Contadores' de este documento. El funcionamiento del dispositivo de juego podrá continuar hasta que los datos críticos sean sobre escritos y perdidos. Debe existir un método para comprobar si existe corrupción de dichas ubicaciones de alojamiento de datos.

2.1.4.1 Chequeos Comprensivos. Se realizarán chequeos comprensivos de la memoria crítica del elemento de interfaz durante cada reanudación de fuerza eléctrica (esto incluye el reinicio del elemento de interfaz).
a) A partir de la reanudación, la integridad de toda la memoria crítica del elemento de interfaz será chequeada.
b) Se recomienda que la memoria crítica del elemento de interfaz sea monitoreada continuamente para detectar la corrupción o con chequeos comprensivos ocurriendo al comienzo de jugar un juego.
c) En adición, se recomienda que el programa de control (software que opera las funciones del elemento de interfaz) permita que el elemento de interfaz continuamente asegure la integridad de todos los componentes del programa de control alojados en la memoria no-volátil.

2.1.4.2 Requisitos del Elemento de Interfaz para el Apoyo de Boletos fuera de línea. Se recomienda que el conjunto de requisitos mínimos a continuación deban ser cumplidos para un elemento de interfaz para que sea capaz de proporcionar información de validación a un dispositivo de juego electrónico para la emisión de vales fuera de línea después de que una pérdida de comunicación ha sido identificada con el sistema de validación de

Boletos/Vales.

a) Se recomienda que el elemento de interfaz sea capaz de comunicarle al juego que la emisión de vales fuera de línea es apoyado y permitir que el juego negocie no apoyar esta facción.
b) Se recomienda que el elemento de interfaz cumpla con los requisitos de la Autentificación Manual de Identificación de la sección 4.2.2.1
c) Se recomienda que el elemento de interfaz limite la cantidad de números de validación y semillas, llave, etc. proporcionadas, valores utilizados para la emisión de vales fuera de línea a un máximo de 25 pares no utilizados.
    i. El elemento de interfaz no le proporcionará a un dispositivo de juego electrónico más de 25 números de validación y semillas, llave, etc. valores permitidos para la emisión de vales fuera de línea hasta que toda información de los vales fuera de línea pendientes haya sido completamente comunicada al sistema de validación de boletos/vales.
d) Se recomienda que el elemento de interfaz fije una duración de expiración máxima de no más de 30 días de juego para todo proporcionado y los números de validación y semillas, llave etc. valores aun no utilizados.
    i. Valores de números de validación y semillas, llave, etc. expirados deben ser desechados de una manera que prevenga el reuso de valores de combinaciones únicas de números de validación y semillas, llave etc. por un período de tiempo suficiente en el sistema.

2.1.5 Requisitos de la Dirección Informática. El elemento de interfaz debe de permitir la asociación de un número de identificación único para que sea utilizado en conjunto con un archivo de las máquinas de juego en el "SMC" Este número de identificación será utilizado por el "SMC" para rastrear toda la información obligatoria de la máquina de juego electrónica asociada. Adicionalmente, el "SMC" no permitirá una entrada duplicada del dato relacionado al número de identificación.

2.1.6 Requisitos del Acceso a la Configuración. El menú o los menús de fijación/configuración del elemento de interfaz no serán disponibles a no ser que se utilice un método de acceso autorizado.

2.2 Requisitos del Procesador Frontal y el Colector de Datos.

2.2.1 Declaración General. Un "SMC" podrá poseer un procesador frontal (en Ingles: front end processor) que recoja y transmita todos los datos desde los colectores de datos conectados, hacia la o las bases de datos asociadas. Los colectores de datos, a su vez, colectarán todos los datos de las máquinas de juego conectadas. La comunicación entre los componentes debe ser a través de un método aprobado y por lo menos deben cumplir con los requisitos de protocolos de comunicación estipulados en la sección 3.1 de este documento. Si el procesador frontal mantiene información en memoria intermedia (buffered) o en un diario, entonces un medio deberá existir para prevenir la pérdida de información critica contenida aquí dentro.

2.3 Requisitos del Servidor y La Base de Datos

2.3.1 Declaración General. Un "SMC" debe de poseer un Servidor o Servidores, sistema conectado a una red o sistemas distribuidos que dirijan el funcionamiento global y una base o bases de datos asociadas que almacenen toda la información ingresada y coleccionada del sistema.

2.3.2 Reloj del Sistema. Un "SMC" debe mantener un reloj interno que refleje la hora actual (en formato de 24 horas - que se comprenderá como el formato local de fecha y hora) y la fecha que será utilizada para proveer lo

siguiente:

a) Sellado de tiempo (en Ingles: time stamping) de los eventos significativos;
b) Reloj de referencia para informes; y
c) Sellado de tiempo (en Ingles: time stamping) de los cambios de configuración.

2.3.3 Facción de Sincronización. Si relojes múltiples son apoyados, el "SMC" tendrá la habilidad con la cual podrá actualizar todos los relojes en los componentes del "SMC" en casos donde conflicto de información pueda ocurrir.

2.3.4 Acceso a La Base de Datos. El "SMC" no tendrá ninguna habilidad integrada con la cual permita a un usuario/operador que desvíe la auditoría del sistema para modificar la base de datos directamente. Los operadores de casinos mantendrán un control de acceso asegurado.

2.4 Requisitos de la Estación de Trabajo

2.4.1 Funcionalidad del Relleno/Premio Gordo (jackpot/Fill). Un Sistema "SMC" debe tener una aplicación o la habilidad de capturar y procesar todos los mensajes de pagos manuales de cada máquina de juego electrónica. Los mensajes de pagos manuales deberán crearse para las ganancias individuales de premios gordos (jackpot), premios gordos progresivos y pagos de créditos acumulados (créditos cancelados), que resulten en pagos manuales. Un relleno (depósito de un monto de monedas/fichas predeterminadas, o de lo contrario apropiadamente autorizada dentro de una tolva en la máquina de juego electrónica) es normalmente iniciado por un mensaje de 'tolva vacía' mientras un crédito cancelado (el retiro de monedas/fichas en exceso desde un dispositivo de juego electrónico) es normalmente iniciado por un usuario. Una excepción admisible al inicio de relleno sería cuando el sistema provea una funcionalidad preventiva o de mantenimiento del relleno, en la cual la transacción podrá ser iniciada por el sistema o por un usuario autorizado. Una vez capturada, deberá haber controles de acceso adecuados para permitir la autorización, alteración o el borrado de cualquier valor previo a su pago o ejecución.

2.4.2 El Límite del Impuesto Reportado. Cada mensaje de pago manual de ganancia individual confirmada por esta aplicación del "SMC" y por personal que tenga la debida autorización, que sea igual o mayor que el límite definido por el país, tendrán que ser reportados. Se requiere que el jugador sea notificado de la necesidad de que se procese un formulario numero/nombre, ya sea a través del "SMC" o manualmente. Esta opción no será capaz de ser sobre escrita. La habilidad de restablecimiento con llave para regresar las ganancias de un evento sujeto a impuestos a un dispositivo de juego debe requerir la intervención de un asistente que anule el recibo original del premio gordo (jackpot) que fue generado.

2.4.3 Información del Recibo del Relleno/Premio Gordo (Jackpot/Fill). La siguiente información será requerida para todos los recibos generados con algunos o todos los detalles de información completados por el "SMC":

a) Tipo de recibo;
b) Identificador numérico del recibo (el cual se incrementa por cada evento);
c) La fecha y la hora;
d) Código de identificación de la máquina de juego;
e) Denominación;
f) Cantidad del relleno;
g) Las cantidades del premio gordo (jackpot), Crédito acumulado y Pago adicional;
h) La indicación del formulario de impuesto (si es aplicable);

i) Pago adicional (si es aplicable);
j) El total en bruto, siendo el total antes de restarle los impuestos y el total de los impuestos(si es aplicable);
k) La cantidad para el jugador;
l) El total de monedas jugadas y el resultado del juego que premió;
m) Las lecturas de los contadores electrónicos; y
n) Firmas de verificación (huellas) de acuerdo a las exigencias de la comisión regulatoria.

NOTA: Lo especificado en los puntos "b" hasta "f", "m" y "n" aplican a los recibos de rellenos y los puntos "b" hasta "e" y "g" hasta "n" aplican a los recibos de premio gordo (jackpot). La información susodicha puede variar dependiendo en los controles internos jurisdiccionales establecidos por la comisión regulatoria y podrán o no podrán ser exigidos.

2.4.4 Funcionalidad de Vigilancia y de Seguridad. Un "SMC" proporcionará un programa de interrogación que permita una búsqueda comprehensiva en-línea del registro de los eventos significativos en el presente y para los catorce (14) días previos, a través de datos archivados o la restauración de la copia de respaldo (backup) cuando el mantenimiento de dichos datos en una base de datos en vivo se estime inapropiado. El programa de interrogación tendrá la habilidad de realizar una búsqueda basada en por lo menos lo siguiente:

a) Rango de fecha y hora;
b) Número de identificación exclusivo del elemento de interfaz/dispositivo de juego y
c) Numero/Identificador del evento significativo.

2.4.5 Funcionalidad Gerencial del Dispositivo de juego Un "SMC" deberá tener un archivo maestro de máquinas de juego (slot file), que consistirá de una base de datos de todas las máquinas de juegos en funcionamiento, incluyendo como mínimo la siguiente información para cada inscripción. Si el "SMC" adquiere cualquiera de estos parámetros directamente de la máquina de juego, deberán existir controles suficientes para asegurar la precisión de la información.

a) Número de identificación exclusivo del elemento de interfaz/localización;
b) Número de identificación de la máquina de juego según asignada por la sala de juego;
c) La denominación de la máquina de juego (Por favor anote que la denominación puede reflejar un valor alternativo, en el caso de un juego de denominaciones múltiples);
d) La retención teórica de la máquina de juego; y
e) El o los programas de control instalados dentro de la máquina de juego.

2.4.6 Funcionalidad de Contabilidad. Un "SMC" debe tener una aplicación o la habilidad de permitir accesos controlados a toda la información de contabilidad (financiera) y será capaz de generar todos los informes obligatorios especificados en la sección titulada "*Requisitos Para la Generación de Informes"* de este documento y también todos los informes requeridos por los controles internos especificados y implementados por la comisión regulatoria.

2.4.7 Exclusiones. Generalmente, cualquier sistema o componente que no se encuentre especificado en el presente documento que impacte el reportar información de ingresos/ganancias deberá ser sometido a un laboratorio de pruebas y certificador para ser ensayado. Por ejemplo, los sistemas de Rastreo de Jugadores independientes (en Ingles: stand alone player tracking) no requieren que sean solicitados, a no ser que sus funciones incluyan una facción o facciones empotradas que afectan los ingresos. (Sin embargo, podrán ser ensayadas, dado a su funcionamiento correcto y el control de versión, cuando se trate de una facción integrada en un SMC siendo solicitada).

CAPITULO 3

3.0 REQUISITOS DEL SISTEMA

3.1 Protocolos de Comunicación

3.1.1 Declaración General Un "SMC" debe apoyar un protocolo o protocolos definidos de comunicación que funcionen como indicado por el o los protocolos de comunicación. Un "SMC" debe proporcionar lo siguiente:

a) Toda las comunicaciones de datos críticos serán basadas en el protocolo y/o incorporar un esquema para la detección y corrección de errores para asegurar una precisión al nivel de noventa y nueve por ciento (99%) o más, de todos los mensajes recibidos;
b) Toda comunicación de datos críticos que puedan afectar los ingresos y que se encuentre desasegurada ya sea por medio de su transmisión o su implementación deberá emplear encriptación. El algoritmo de encriptación debe emplear claves variables o una metodología similar para preservar la seguridad de las comunicaciones; y
c) Toda comunicación realizada dentro del sistema, en su totalidad, debe funcionar precisamente de acuerdo a lo indicado por el protocolo de comunicación implementado.

3.2 Eventos Significativos

3.2.1 Declaración General. Los eventos significativos se generan por un dispositivo de juego y se envían a través del elemento de interfaz al "SMC" utilizando un protocolo de comunicación aprobado. Cada evento deberá ser almacenado en una o más bases de datos que incluya lo siguiente:

a) La fecha y hora en que ocurrió el evento; y
b) La identidad de la máquina de juego que generó el evento; y
c) Un numero/código exclusivo que defina el evento; o
d) Un texto breve que describa el evento en el lenguaje local.

3.2.2 Eventos Significativos. Los siguientes eventos significativos deberán ser coleccionados desde la máquina de juego y transmitidos al sistema para su almacenamiento:

a) Restauración o falla de la corriente eléctrica;
b) Condiciones de pagos manuales (es necesario que la cantidad sea enviada al sistema):
    i. El premio gordo (jackpot) de la máquina de juego (un premio singular que exceda el límite de una ganancia en la máquina de juego);
    ii. El pago manual de créditos cancelados; y
    iii. El premio gordo (jackpot) progresivo (según el premio gordo mencionado anteriormente).
c) Aperturas de puertas (cualquier puerta que permita el acceso a un área crítico de la máquina de juego. Conmutadores de Puerta (ingresos distinguibles al elemento de interfaz) son aceptables a condición que su operación no resulte en mensajes redundantes o confusos.
d) Errores de Monedas o Fichas ingresadas (Es aceptable reportar Moneda Atascada Ingresada, Moneda Ingresada en reverso y Moneda demasiada lenta como un error de Moneda Ingresada genérico);
e) Errores de verificador de billetes (articulo/ítem) (los siguientes puntos "i" y "ii" deben de ser enviados como mensajes exclusivos, si apoyado por el protocolo de comunicación):

i. Apilador lleno (se recomienda que un mensaje de error explícito de Apilador Lleno no sea utilizado, dado que puede promocionar un asunto de seguridad, más bien seria un mensaje de "Malfuncionamiento del Verificador de Billete" o equivalente); y
ii. Billete atascado (objeto).

f) Error de la Batería de RAM Baja de Carga en la máquina de juego;
g) Errores de rodillos girantes (si es aplicable, el número específico del rodillo deberá identificarse en el código de error);
h) Errores de Monedas o Fichas entregadas (Deben de ser enviados como mensajes exclusivos, si apoyado por el protocolo de comunicación):
   i. Atasques en la tolva;
   ii. Tolva descontrolada o monedas adicionales pagadas; y
   iii. Tolva vacía.
i) Errores de impresora (si apoyan una impresora):
   i. Papel Vacío o poco papel; y
   ii. Impresora desconectada/fallo.

3.2.3 Eventos de Prioridad Genéricos. Los siguientes eventos significativos deben de ser transmitidos al "SMC" y deberá existir un mecanismo para la notificación puntual (es permisible que los siguientes eventos significativos sean enviados al sistema como un código de error genérico) en los casos que la máquina de juego no pueda distinguir los detalles del evento:

a) Perdida de Comunicación con el Elemento de Interfaz;
b) Perdida de Comunicación con el Dispositivo de Juego;
c) Corrupción en la memoria del elemento de interfaz (si esta almacenando información critica); y
d) Corrupción de la memoria RAM de la máquina de juego.

3.3 Contadores

3.3.1 Declaración General. La información de los contadores se genera en la máquina de juego y coleccionada por el elemento de interfaz y enviada al "SMC" a través de un protocolo de comunicación. Esta información podrá ser leída directamente desde la máquina de juego o podrá ser transmitida utilizando una función delta. La información de contadores en el "SMC" será identificada de tal forma que puedan ser entendidos claramente de acuerdo a su función.

3.3.2 Contadores Exigidos. La siguiente información de contadores deberá ser comunicada desde la máquina de juego y almacenada en el sistema en unidades igual a la denominación de la máquina de juego o en dólares y centavos:

a) Coin In (Moneda Ingresada):
   i. El sistema mantendrá la información proporcionada por la máquina de juego de las monedas ingresadas de las tablas de pago y el porcentaje de retorno teorético de cada juego múltiple o de denominación múltiple/juego múltiple.
   ii. El sistema mantendrá la información proporcionada por cada máquina de juego de las monedas ingresadas por tabla de pago y la información sobre el promedio balanceado (en Ingles: weighted average) del porcentaje de retorno teórico para las tablas de pago con diferencias en el porcentaje de retorno teórico que excedan cuatro (4%) por ciento entre las categorías de apuesta.

NOTA: Esto no aplica a los juegos Keno o de Habilidad.

b) Coin Out (Moneda Entregada);
c) Total Coin Drop (Total de Moneda Caída). Las monedas desviadas a la caja de caída o un total de todas las monedas, billetes y boletos/vales desviados;
d) Attendant Paid Jackpots (Pagos de Premios por Asistente). Pagos manuales;
e) Attendant Paid Cancelled Credits (Créditos Cancelados Pagados por asistente) (si es apoyado por la máquina de juego);
f) Physical Coin In (Moneda Física Ingresada);
g) Physical Coin Out (Moneda Física Entregada);
h) Bill In (Billete Ingresado). El valor total de todos los billetes aceptados;
i) Ticket/Voucher Out (Boleto/Vale Entregado). El valor total de todos los boletos/vales emitidos;
j) Machine Paid External Bonus Payout (Pago de Bonificación Externo Pagado por la Maquina);
k) Attendant Paid External Bonus Payout (Pago de Bonificación Externo pagado por asistente);
l) Attendant Paid Progressive Payout (Premio Progresivo Pagado por Asistente);
m) Machine Paid Progressive Payout (Pago Progresivo Pagado por la Maquina);
n) Ticket/Voucher In (Boleto/Vale Ingresado). El valor total de todos los boletos/vales aceptados.

NOTA: Por favor refiérase a los estándares GLI-11 relativo a los contadores que deberán de estar mantenidos por la máquina de juego. Mientras que estos contadores electrónicos de contabilidad deberán ser comunicados directamente desde la máquina de juego al "SMC", será aceptable la utilización de calculaciones secundarias en el "SMC" cuando sea apropiado.

3.3.3 Borrado de Contadores. Un elemento de interfaz no podrá tener un mecanismo por el cual un usuario desautorizado pueda causar la pérdida de ninguna información almacenada de los contadores de contabilidad, refiérase a la sección titulada "*El Búfer de Información*".

3.4 Requisitos para la Generación de Informes

3.4.1 Declaración General. La información de eventos significativos y de contadores se almacena en el "SMC" en una base de datos y los informes de contabilidad son subsiguientemente generados por medio de efectuar una búsqueda sobre la información almacenada.

3.4.2 Informes Requeridos. Los informes serán generados de acuerdo a un itinerario determinado por la comisión regulatoria, cual típicamente consiste de informes de épocas diarias, mensuales, anuales y vitales generados a partir de la información almacenada en la base de datos. Estos informes como mínimo consistirán de lo siguiente:

a) Reporte de Ganancia neta/Ingreso para cada máquina de juego;
b) Reporte de comparación de caídas por cada medio desviado a la caja de caída (por ejemplo, monedas, billetes) con las variaciones del valor monetario y el porcentaje por cada medio y el acumulado por cada tipo;
c) Reporte de comparación entre lo que fue contabilizado como premios gordos (jackpot) y el valor actual con las variaciones del valor monetario y el porcentaje por cada premio gordo y el acumulado;
d) Reporte de comparación entre la retención teórica y la retención actual con sus variaciones;
e) Reporte de eventos significativos para cada máquina de juego electrónica; y
f) Otros reportes, que pudieran ser requeridos por la comisión regulatoria.

NOTA: Es aceptable que los datos en los reportes se combinen cuando sea apropiado (por ejemplo: Ingresos, comparación teórica/actual)

NOTA: Para requisitos adicionales de informes cuando las máquinas de juegos apoyando caídas de boletos/vales sean interconectadas por favor refiérase a la sección titulada "REQUISITOS PARA LOS SISTEMAS DE VALIDACIÓN DE BOLETOS/VALES" de este documento.

3.5 Requisitos de Seguridad

3.5.1 Control de Acceso. El "SMC" deberá apoyar ya sea una estructura jerárquica de personificación por la cual el nombre del usuario y la contraseña definen el acceso a los programas o a las opciones en particular de menús o bien, admitirá la entrada de acceso (en Ingles: login) a programas y dispositivos aseguradamente, basándose estrictamente en el nombre del usuario y contraseña o Número Personal de identificación (PIN). Además, el "SMC" no permitirá ninguna alteración del registro de información significativa que haya sido comunicada desde la máquina de juego. Adicionalmente, deberá existir una provisión para notificar al administrador del sistema y para el bloqueo de usuarios o una entrada en el registro de auditoría, cuando ocurra un número determinado de intentos de entradas de acceso fracasadas.

3.5.2 Alteración de Datos. El "SMC" no permitirá la alteración de ninguna información de contabilidad o del registro de eventos significativos que haya sido apropiadamente comunicada desde la máquina de juego sin tener controles de acceso supervisados. En casos que se cambie algún dato financiero, un registro automatizado de auditoría deberá ser capaz de ser producido para documentar:

a) El dato alterado;
b) El valor del dato previo a la alteración;
c) El valor del dato después de la alteración;
d) La hora y fecha de la alteración; y
e) El usuario que realizó la alteración (Entrada de acceso del usuario).

3.6 Facciones Adicionales del Sistema

3.6.1 Requisitos para la Verificación de Programas del Dispositivo de juego. Cuando sea apoyado, un "SMC" podrá proveer esta funcionalidad redundante para verificar el software del juego de la máquina de juego. Aunque el esfuerzo involucrado puede potencialmente impedir las operaciones de la máquina de juego y el "SMC", la siguiente información deberá ser verificada para su validez, previamente a la implementación:

a) Algoritmo(s) de firmas del software; y
b) Algoritmo(s) de verificación de errores en la comunicación de datos.

NOTA: El estándar susodicho está sujeto un a repaso basado en regulaciones jurisdiccionales que podrán ser o no ser exigida del "SMC".

3.6.2 Ocasiones Requeridas del Algoritmo de Verificación. La verificación podrá ser iniciada por usuario o iniciada por evento(s) significativo(s) específico(s) en la máquina de juego. Para asegurarse un alcance completo, la verificación deberá ser realizada después de cada uno de los siguientes eventos:

a) El encendido de la máquina de juego; y
b) La instalación de una nueva máquina de juego.

NOTA: El estándar susodicho está sujeto a un repaso basado en regulaciones jurisdiccionales que podrán ser o no ser exigida del "SMC".

3.6.3 Requisitos de Descargas FLASH. Cuando sea apoyado, un "SMC" podrá utilizar tecnología FLASH para instalar el software del elemento de la interfaz, a condición que cumpla con todos los requisitos a continuación:

a) La funcionalidad de Descargas FLASH deberá, como mínimo, contar con protección de contraseña a un nivel de supervisor. El "SMC" podrá continuar localizando y verificando versiones que estén funcionando en el presente momento, pero no podrá cargar código (programas) que no estén funcionando en el presente momento en el sistema sin la intervención del usuario;
b) Un registro de auditoría debe registrar la hora y fecha de una descarga FLASH y alguna provisión deberá efectuarse para asociar este registro con: cual versión o versiones del código que fue descargado y el usuario que inició la descarga. Un reporte separado del registro de auditoría de descarga Flash sería lo ideal.
c) Todas las modificaciones de los ejecutables o archivos flash descargables deberán presentarse a un laboratorio de ensayos y certificador para su aprobación. El laboratorio de ensayos realizará una descarga FLASH al sistema existente en el laboratorio de ensayos y verificará su operación. Después, el laboratorio de ensayos le asignará firmas electrónicas a los códigos ejecutables y archivo(s) flash que sean relevantes, para que puedan ser verificados por un regulador en las salas de juego. Adicionalmente, todos los archivos flash deberán estar disponibles a un regulador para poder verificar la firma.

NOTA: Lo susodicho se refiere exclusivamente a las instalaciones de nuevos códigos ejecutables. Otros parámetros de programa podrán ser actualizados a condición que el proceso sea firmemente controlado y sujeto a una auditoría.

3.6.4 Requisitos para el Acceso Remoto. Cuando apoyado, el "SMC podrá utilizar acceso remoto controlado por contraseña para lograr el acceso al "SMC" a condición que cumplan con los siguientes requisitos:

a) Un registro de actividad de usuarios de acceso remoto será mantenido que describa el nombre de entrada de acceso (en Ingles: login) del usuario, la fecha y hora, duración y la actividad desarrollada durante el acceso;
b) No se permitirán funcionalidades administrativas sin autorización por usuarios remotos (por ejemplo, agregando usuarios, cambiando permisos, etc.);
c) No se permitirá el acceso sin autorización a la base de datos, que no sea retiros de información por medio de la utilización de funciones existentes;
d) No se permitirá el acceso sin autorización al sistema operativo; y
e) Si el acceso remoto es de ser constantemente, entonces se deberá instalar un filtro de red (firewall) para prevenir el acceso no autorizado.

NOTA: Se reconoce que el fabricante del "SMC" podrá acceder al "SMC" de forma remota y a sus componentes asociados con el propósito de apoyar el producto y los usuarios, según sea necesario. Sin embargo, esta facción deberá ser opcional y lograse por un medio asegurado para acomodar a las jurisdicciones que no permiten el acceso remoto.

3.6.5 Verificación del Software del Sistema

Los componentes/módulos del software del Sistema serán verificables por un método asegurado (como está definido en la sección titulada "Control de Acceso" de este documento) al nivel del sistema, denotando el

numero/código de identificación del programa y versión. El sistema tendrá la capacidad de permitir una verificación de integridad de los componentes/módulos independientemente por medio de un método externo y será requerido para todos los programas de control que puedan afectar la integridad del sistema. Esto podrá lograrse por medio de ser autenticado por un dispositivo de un tercer partido, cual podrá estar empotrado dentro del software del sistema o teniendo un puerto de interfaz para un dispositivo de un tercer partido que autentique el medio. Esta verificación de integridad proporcionará un medio para las verificaciones de los componentes/módulos del sistema en las salas de juego con el propósito de identificar y validar los programas/archivos. Previo a la aprobación del sistema, el laboratorio de ensayos y certificador aprobará el método de verificación de integridad.

NOTA: Si el programa de autenticación esta contenido dentro del software del sistema, el fabricante debe de recibir una aprobación por escrito del laboratorio de pruebas previamente a la sumisión.

3.7 Copias de Respaldo y Restauración

3.7.1 Declaración General. El "SMC" tendrá la suficiente redundancia y modularidad de manera que si algún componente individual falla o parte de un componente falla, los juegos puedan continuar. Habrá copias redundantes de cada archivo de registro o base de datos del sistema o ambos en el "SMC" con soporte abierto para las copias de respaldo y restauración.

3.7.2 Requisitos para la Restauración. En caso de un evento de fallo catastrófico cuando el "SMC" no se pueda reiniciar de ninguna otra manera, será posible restablecer el sistema a partir del último punto viable de la copia de respaldo y completamente recuperar los contenidos de la copia de respaldo, recomendándose que consista de la siguiente información como mínimo:

a) Eventos significativos;
b) Información de contabilidad;
c) Información de auditoría;
d) Información específica a la sala de juego, tal como el archivo de las máquinas tragamonedas, archivos de empleados, configuraciones progresivas, etc; y
e) Si se apoya la emisión de vales, toda información utilizada en el proceso de redención de vales incluyendo la información específica a la redención de vales fuera de línea, si corresponde.

CAPITULO 4

4.0 REQUISITOS PARA LOS SISTEMAS DE VALIDACIÓN DE BOLETOS/VALES

4.1 Introducción

4.1.1 Declaración General. Un sistema de validación de boletos/vales puede ser completamente integrado en un Sistema Monitoreo y de Control (SMC) o puede existir como una entidad completamente separada. Sistemas de Validación de boletos/vales son generalmente clasificados en (2) dos tipos: Sistemas de boletos/vales bidireccionales que permiten los dispositivos de juegos imprimir y redimir boletos/vales (TITO) y Sistemas de solo emisión de boletos/vales (TOO) que permiten los dispositivos de juegos imprimir boletos/vales pero no permiten la redención de boletos/vales. Este capítulo primariamente atiende sistemas bidireccionales de boletos/vales. Cuando los sistemas de boletos/vales de solo emisión son utilizados, algunos de lo siguiente quizás no aplique.

4.1.2 Pago por Impresora de Boletos/Vales Pago por impresora de boletos/vales como método de redención de créditos en un dispositivo de juego es solamente permitido cuando la máquina de juego esté enlazada con a un Sistema de Validación aprobado o un "SMC" que permita la validación del boleto/vale impreso. La información de validación vendrá del sistema de validación o "SMC" que utilice un protocolo de comunicación asegurado.

NOTA: Para el apoyo de emisión de vales fuera de línea, el dispositivo de juego debe estar enlazado a un sistema de validación aprobado o un "SMC" que permita validación de los boletos/vales impresos, pero que no tenga que estar constantemente comunicándose para la emisión de boletos para ser permisible.

4.2 Emisión de Boleto/Vale

4.2.1 Información Utilizada por la Dispositivo de juego de un Boleto/Vale Mientras se está Comunicando con un Sistema de Validación.

El sistema de validación de boletos/vale deberá ser capaz de comunicar los siguientes datos a la máquina de juego para imprimirlos en el boleto/vale.

a) Nombre de La Sala De Juego/Identificador del Lugar;
b) La indicación de un periodo de expiración a partir de la fecha de emisión, o la fecha y hora que el boleto/vale se expirará, cuando sea aplicable (en formato de veinticuatro (24) horas lo cual es entendido como el formato de fecha/hora local);
c) Fecha y Hora del Sistema (en formato de veinticuatro (24) horas lo cual es entendido como el formato de fecha/hora local); y
d) El número de validación para que la máquina produzca el número de validación en el boleto/vale.

4.2.2 Algoritmos para Generar Números de Validación o Semillas de Boletos/Vales.

a) **Validación en el Sistema** – El algoritmo o método utilizado por el sistema de validación o "SMC" para generar el número de validación de un boleto/vale debe garantizar un porcentaje insignificante de números de validación repetidos.

b) **Numero de Validación Generado por la Dispositivo de juego (semilla del sistema) -** El sistema de validación deberá enviar una semilla exclusiva a la máquina de juego cuando matricule la máquina de juego como capaz de imprimir boletos/vales. El sistema con posterioridad podrá enviar una semilla nueva a la máquina de juego después que el boleto/vale haya sido impreso. El algoritmo o métodos utilizados para determinar la semilla deberá garantizar un porcentaje insignificante de números de validación repetidos.

4.2.2.1 Algoritmo para Generar Boletos/Vales fuera de Línea Identificadores de Autentificación.

Cuando apoyado, el identificador de autentificación fuera de línea debe ser de un valor exclusivo que sea derivado por un método de generar claves o llaves (HASH) u otro método de encriptación asegurado de por lo menos 128 bits, el cual podrá exclusivamente identificar el instrumento de apuesta, verifique que el sistema de redención también fue el sistema de emisión y valide el monto del vale. Los siguientes conjuntos mínimos de entrada de datos deben ser utilizados para crear el identificador de autentificación:

a) Identificador de el dispositivo de juego;
b) Numero de validación;
c) Monto del Vale; y
d) Semilla asegurada, llave, etc. proporcionado por el sistema de validación o el "SMC" al dispositivo de juego.
   i) Semillas aseguradas, llaves, etc. como asignadas deben de ser suficiente aleatorias. Medidas para evitar predictibilidad serán evaluadas por el laboratorio de pruebas caso por caso.
   ii) La longitud mínima para cualquier semilla asegurada, llave, etc. implementada por el sistema de validación o "SMC será escogido de un grupo de tipo variable especificado por el protocolo de comunicación utilizado. El grupo debe ser compuesto de por los menos 10 elevado a la potencia de 14 (10^{14}) de valores aleatoriamente distribuidos.

4.2.3 Registros del Sistema de Boletos/Vales.

a) El sistema de validación deberá recoger la información de Boletos/Vales correctamente basada en el protocolo de comunicación asegurado implementado, y almacenar la información de boletos/vales dentro de una base de datos.
b) El registro del boleto/vale en el sistema anfitrión deberá contener por lo menos la siguiente información de los boletos/vales:
   1. Numero de Validación;
   2. La fecha y hora que la máquina de juego imprimió el boleto/vale (en formato de veinticuatro (24) horas la cual es entendida como el formato de fecha/hora local);
   3. Tipo de transacción u otro método de diferenciar los tipos de boletos/vales (presumiendo que múltiples tipos de boletos/vales son disponibles);
   4. El valor numérico en dólares y centavos del boleto/vale;
   5. El estado del boleto/vale (es decir, válido, sin redimir, pendiente, nulo, inválido, redención en progreso, redimido, etc.)
   6. La fecha y hora que el boleto/vale se expirará (en formato de veinticuatro (24) horas lo cual es entendido como el formato de fecha/hora local o un periodo de expiración a partir de la fecha de emisión);
   7. Numero de la máquina (o numero de localización de la Caseta de Cajera/Cambio, si la creación de boletos/vales fuera de la máquina de juego es apoyado) que identifique de donde fue emitido el boleto/vale.

4.2.4 Requisitos del Sistema para el Apoyo de Boletos Fuera de Línea. Esta sección es recomendada cuando una rutina de boletos fuera de línea aprobada es apoyada.

a) Apoyar la identificación y redención de boletos fuera de línea a través de una aplicación proporcionada por sistema.
b) Registrar todo acceso y operaciones de usuarios de la aplicación susodicha por 14 días a través de datos archivados o la restauración de copias de respaldos cuando el mantenimiento de dichos datos en una base de datos en vivo es considerada inapropiada.
c) El sistema de validación o "SMC" debe fijar un plazo de expiración máximo que no sea mayor de 30 días de juegos para todos los valores proporcionados y los números de validación, semillas, llaves, etc. no utilizados.
d) Los valores de números de validación expirados, semillas, llaves etc. deben ser descartados de manera que impida el re-uso de valores en combinaciones exclusivas de números de validación, semillas, llaves, etc. por un periodo de tiempo suficiente en el sistema.

4.2.5 Impresión de Boletos/Vales Durante una Pérdida de Comunicación con el Sistema de Validación.
Para los sistemas de validación que se comunican con la máquina de juego a través de un SMIB (Tablero de interfaz Sistema Máquina) si cualquier enlace entre el SMIB y el "SMC" pierden conexión, el SMIB tendrá que:

a) No responderle a la petición de validación de la máquina de juego y suspender la impresión de boletos/vales, o
b) Impedir que la máquina de juego continúe emitiendo más boletos/vales, o
c) No leer o almacenar más ninguna información de boletos/vales generada por la máquina de juego.

NOTA: Un máximo de dos (2) boletos/vales serán aceptables inmediatamente después de una pérdida de comunicación, en casos donde el elemento de interfaz ya haya recibido la semilla por el sistema, a condición que la información de emisión del boleto/vale sea enviada inmediatamente cuando la comunicación se restablezca.

NOTA: Esta sección no aplica a sistemas utilizando una rutina aprobada de vales fuera de línea.

4.3 Redención de Boletos/Vales

4.3.1 Redención de Boletos/Vales en Línea. Los boletos/vales podrán ser redimibles en máquinas de juego, casetas de cajera/cambio u otros terminales de validación (kioscos) aprobados, a condición que estén matriculadas para la validación de boletos/vales con un sistema de validación. También refiérase al estándar GLI-11 sección 2.31 para los requisitos de los dispositivos de juegos con respecto a la validación de boletos/vales.

a) El sistema de validación tendrá que procesar la redención de boletos/vales correctamente de acuerdo al protocolo de comunicación asegurado implementado;
b) El sistema de validación tendrá que actualizar el estado del boleto/vale en la base de datos durante cada etapa del proceso de validación en conformidad. En otras palabras, en cualquier momento que cambie el estado del boleto/vale, el sistema tendrá que actualizar la base de datos, bajo cada cambio de estado, la base de datos deberá indicar la siguiente información:
    1. La fecha y hora del cambio de estado;
    2. El estado del boleto/vale;
    3. El valor del boleto/vale;
    4. Numero de la máquina o la identificación de origen que identifique de donde vino la información del boleto/vale.

4.3.2 Redención del Boletos/Vales Fuera de Línea. Cuando apoyado, los Boletos/Vales pueden ser redimidos

en una caja de cajero/cambio a condición que esté matriculada con un sistema de validación para validar boletos/vales.

a) El sistema de validación como mínimo debe apoyar la identificación y redención de vales fuera de línea a través de una aplicación proporcionada por sistema;

b) El sistema de validación debe procesar la redención de boletos/vales correctamente de acuerdo al protocolo de comunicación asegurado implementado;

c) El sistema de validación debe actualizar el estado del boleto/vale en la base de datos durante cada etapa del proceso de redención como corresponde. En otras palabras, cada vez que el estado del boleto/vale cambie, el sistema debe actualizar la base de datos. Sobre cada cambio de estado, la base de datos debe indicar la siguiente información:

i) Fecha y hora del cambio de estado;
ii) Estado del boleto/vale;
iii) Valor del boleto/vale;
iv) Número de la máquina o identificación de origen de donde vino la información del boleto/vale.

4.3.3 Operación de la Caseta de Cajera/Cambio. Todos los terminales de validación deberán ser controlados por nombres de usuarios y contraseñas. Cuando se presente un boleto/vale para redención, la cajera deberá:

a. Escanear el código de barra a través de un lector óptico o su equivalente; o
b. Manualmente ingresar el dato del número de validación del boleto/vale; y
c. Podrá imprimir un recibo de validación, después de que el boleto/vale sea electrónicamente validado, cuando sea aplicable.

4.3.4 Información del Recibo de Validación. Cuando sea aplicable, el recibo de validación, como mínimo, contendrá la siguiente información impresa:

a) Número de la máquina;
b) Número de validación;
c) La fecha y hora en que se pagó;
d) El Monto; y
e) Identificación de la Caseta de Cajera/Cambio.

4.3.5 Notificación de Boleto/Vale Inválido. El sistema de validación o "SMC" deberá tener la capacidad de identificar estas ocurrencias y notificar la cajera que una de las siguientes condiciones existe:

a. El boleto/vale no se encuentra en el archivo (fecha pasada, falsificado, etc.);
b. El boleto/vale ya ha sido pagado; o
c. El monto del boleto/vale es diferente que el monto archivado (este requisito se podrá cumplir exhibiendo el monto del boleto/vale para su confirmación por la cajera durante el proceso de redención).

4.3.6 Redención de Boletos/Vales Durante Pérdida de Comunicación. En caso que el sistema de datos en línea falle temporalmente y la información de validación no pueda ser enviada al sistema de validación o "SMC", un método alternativo de pago deberá ser proveído ya sea por el sistema de validación posesionando facciones únicas (es decir, verificación de la validez de la información del boleto/vale en conjunción con un almacenamiento de base de datos local), para identificar boletos/vales duplicados e impedir el fraude mediante la reimpresión y la redención de un boleto/vale que haya sido previamente emitido por la máquina de juego; o la utilización de un método aprobado alternativo como designado por la comisión regulatoria que pueda lograr los mismo.

NOTA: Un máximo de dos (2) boletos/vales serán aceptables inmediatamente después de una pérdida de comunicación, en casos donde el elemento de interfaz ya haya recibido la semilla por el sistema, a condición que la información de emisión del boleto/vale sea enviada inmediatamente cuando la comunicación se restablezca.

NOTA: Esta sección no aplica a sistemas utilizando una rutina aprobada de vales fuera de línea.

4.3.7 Terminales de Redención (Kioscos) Refiérase al GLI-20 Terminales de Redención para los estándares técnicos para estos dispositivos.

4.4 Informes

4.4.1 Requisitos de Informes. Los siguientes informes deberán generarse como mínimo y conciliarse con todos los boletos/vales validados/redimidos:

a. Reporte de emisión de boletos/vales;
b. Reporte de redención de boletos/vales;
c. Reporte de obligación financiera de boletos/vales;
d. Reporte de desacuerdo de los boletos/vales caídos;
e. El Reporte detallado de transacción deberá estar disponible en el sistema de validación que muestre todos los boletos/vales generados por un dispositivo de juego y todos los boletos/vales redimidos por el terminal de redención u otra máquina de juego; y
f. El Reporte de Cajera, cual deberá individualmente detallar los boletos/vales, la suma de los boletos/vales pagados por la Caseta de Cajera/Cambio o Terminal de redención.

NOTA: Los requisitos en los puntos (b) y (d) susodichos, serán exentos cuando existan boletos/vales de dos partes en la máquina de juego donde la primera parte es dispensada al jugador como un boleto/vale original y la segunda parte permanece ajuntada al mecanismo de la impresora como una copia (en un rollo continuo) en la máquina de juego.

4.5 Seguridad

4.5.1 Seguridad de los Componentes de la Base de Datos y Validación. Una vez que la información de validación sea almacenada en la base de datos, los datos no podrán ser alterados de ninguna manera. La base de datos del sistema de validación deberán ser encriptados o protegidos por contraseña y deberá tener auditoría del rastreo de usuarios cual no pueda ser alterado para evitar el acceso desautorizado. Más aún, la operación normal de cualquier dispositivo que contenga información de boletos/vales no tendrá ningunas opciones o método que pueda comprometer la información de los boletos/vales. Cualquier dispositivo que contenga información de boletos/vales en su memoria no permitirá la eliminación de la información a no ser que primero haya transferido dicha información a la base de datos u otro componente o componentes asegurados del sistema de validación.

CAPITULO 5

5.0 REQUISITOS AMBIENTALES Y DE SEGURIDAD DE LOS SISTEMAS.

5.1 Introducción

5.1.1 Declaración General. El presente capítulo gobernará los requisitos ambientales y de seguridad para todos los componentes de sistemas sometidos para su evaluación.

5.2 Seguridad del Hardware y el Jugador.

5.2.1 Declaración General. Las piezas eléctricas y mecánicas y diseños principales del hardware electrónico asociado no deberán exponer a un jugador a ningún peligro físico. El laboratorio de pruebas y certificador NO hará ninguna conclusión con respecto a peligros y pruebas de EMC ya que esto es responsabilidad del fabricante de la mercancía o de aquellos que compran la mercancía. Pruebas de peligros y de EMC se pueden requerir bajo estatuto separado, regulación, ley o acto y se debiera investigar cómo le corresponde, por los partidos que fabriquen o compren dicho hardware (soporte físico). El laboratorio de pruebas y certificador no ensayará, no será responsable por, y no hará conclusiones relacionadas a esta materia. Sin embargo, la comisión regulatoria reglamentará estos aspectos de acuerdo a las normas, decretos, resoluciones y leyes vigentes para tal fin.

5.3 Efectos Ambientales Sobre la Integridad del Sistema

5.3.1 Estándar de Integridad. El Laboratorio realizará ciertas pruebas para determinar si existen influencias externas que afecten la imparcialidad al jugador del juego o pueda crear oportunidades de hacer trampa. Un sistema en línea deberá ser capaz de resistir las siguientes pruebas, reasumiendo su función sin la intervención del operador:

a) Interferencia Electro-Magnética. Los sistemas no crearán ruido electrónico que afecte la integridad o imparcialidad de equipo asociado cercano;
b) Interferencia Electro-Estática. La protección contra descargas estáticas requiere que el hardware del sistema estén conectados a tierra de tal manera que la energía por descarga estática no dañe o inhiba el funcionamiento normal de los componentes electrónicos u otros componentes localizados dentro del sistema. Los sistemas podrán exhibir interrupciones temporarias cuando sean sometidos a una descarga electrostática significante, mayor a la que le corresponde al cuerpo humano, pero deben tener la capacidad de recuperase y completar cualquier función interrumpida sin pérdida o corrupción de ningún control o información de datos asociados con el sistema. Las pruebas serán conducidas con un nivel de severidad de hasta 27KV en la descarga de aire.