SCJ | SUPERINTENDENCIA DE CASINOS DE JUEGO

Estándares para Sistemas de Monitoreo y Control en Línea

Superintendencia de Casinos de Juego (SCJ)

CHILE

Santiago de Chile, Julio de 2019

Modificaciones a los Estándares para Sistemas de Monitoreo y Control en Línea

Los Estándares para Sistemas de Monitoreo y Control en Línea fueron aprobados mediante la Resolución Exenta N°623, de fecha 27 de diciembre de 2013, de la Superintendencia de Casinos de Juego, y han sido modificados por:

1. Resolución Exenta N°84 de 1 de abril de 2014, de la Superintendencia.
2. Resolución Exenta N°52 de 20 de marzo de 2015, de la Superintendencia.
3. Resolución Exenta N°219 de 1 de abril de 2019, de la Superintendencia.

Tabla de contenido

1. Introducción.

1.1 Propósito.

El propósito de este documento es definir los requerimientos clave para Sistemas de Monitoreo y Control en Línea (SMC), para su operación en la República de Chile.

Se recomienda que, para obtener una mejor comprensión de este documento, también se lean todas las demás regulaciones aplicables a la actividad de los casinos de juego autorizados en la República de Chile bajo el amparo de la Ley N°19.995 y sus reglamentos.

1.2 Objetivos y principios.

El objetivo de este documento es especificar los requerimientos y controles necesarios para que los equipos y las operaciones del Sistema de Monitoreo y Control en Línea aseguren que los juegos dentro de la República de Chile sean:

1. Seguros,
2. Confiables,
3. Susceptibles de ser auditados.

Los principios que rigen la producción y uso de este estándar son:

1. Las implementaciones alternativas para las especificaciones contenidas en este documento se considerarán caso a caso.
2. Todo hardware o software debe funcionar de acuerdo con los requerimientos de este documento, así como también con los correspondientes al diseño y especificaciones del fabricante.
3. Los equipos de juegos no deben hacer trampas, engañar o dejar a los jugadores en desventaja y no los deben poner en peligro a ellos ni al personal autorizado.

2. Definición de un SMC.

Un Sistema de Monitoreo y Control en Línea (SMC), también denominado Sistema On Line o Sistema de Administración de Máquinas de Azar, es un sistema de administración de juego que monitorea continuamente cada dispositivo de juego electrónico por medio de un protocolo de comunicación específico ya sea por una línea dedicada, por un sistema de conexión por línea conmutada o por cualquier otro método de transmisión asegurada. La tarea principal de un SMC es proporcionar registros de datos, búsquedas e informes de los eventos significativos de juegos, recolección de datos financieros de las máquinas de azar y datos de contadores, reconciliación de los datos de contadores contra los conteos electrónicos actuales y su seguridad.

Cada máquina de azar o dispositivo de juego instalado en una sala de juego, en caso que no realice la función de comunicación, deberá contar con un dispositivo o interfaz instalado en un área segura de la misma, que proporcione la comunicación entre la máquina de azar y el SMC. Será permitido que exista un recolector de datos externos o un controlador de progresivos, los que deberán guiarse por el presente estándar o por aquel que lo complemente.

Todas las máquinas de azar instaladas en las salas de juego deberán estar conectadas a un SMC, debiendo ser registrada en línea la información de las mismas con las excepciones descritas en el presente estándar.

2.1 La Certificación

La aprobación de un SMC será certificada mediante ensayos en un laboratorio, donde éste comprobará la integridad del sistema en conjunto con las máquinas de azar, en un ambiente de laboratorio con el equipo ensamblado.

3. Funcionalidad del SMC

3.1 Requerimientos de configuración

3.1.1 El sistema debe proveer una función para registrar una nueva máquina de azar en forma única.

3.1.2 El elemento de interfaz debe permitir la asociación de un número de identificación único para que sea utilizado en conjunto con un archivo de las máquinas de azar en el SMC. Este número de identificación será utilizado por el SMC para rastrear toda la información obligatoria de la máquina de azar asociada. Adicionalmente, el SMC no permitirá una entrada duplicada del dato relacionado al número de identificación. El sistema no debe permitir duplicación en la creación del campo único de identificación.

3.1.3 El sistema debe poseer un identificador único (p.ej. N° de Serie o N° de Activo) para cada máquina de azar e identificadores asociados del fabricante y del modelo, que no se puedan modificar jamás sin una pista de auditoria, una vez que la máquina de azar haya sido registrada en el sistema.

3.1.4 El sistema podrá tener la capacidad de registrar la información de configuración asociada a una máquina de azar. El acceso a este menú o menús de configuración no deberá ser posible a no ser que se utilice un método de acceso autorizado como por ejemplo nombre de usuario y contraseña.

3.1.5 El sistema debe poseer como mínimo la capacidad de imprimir y/o desplegar la información histórica recolectada de contadores y eventos, basándose en el número de identificación exclusivo de la máquina azar correspondiente.

3.2 Requerimientos de medición.

3.2.1 Se debe almacenar en forma segura los medidores (contadores) o archivos asociados con la información de los jugadores y el juego realizado, por lo que toda alteración a estos registros deberá originar un rastro de auditoria.

3.2.2 Como mínimo, el SMC debe recolectar y almacenar todos los medidores o contadores de todas las máquinas de azar conectados en períodos específicos de tiempo.

El certificado debe dar cuenta del tiempo mínimo en el cual se refresca la información desde los dispositivos de juego y el SMC, así también de si éste es configurado en forma manual o automática.

3.2.3 La información de los contadores que se genera en la máquina de azar y que es recolectada por el elemento de interfaz, debe ser enviada al SMC a través de un protocolo de comunicación. Esta información podrá ser leída directamente desde la máquina de azar o podrá ser transmitida utilizando una función delta. La información de contadores en el SMC deberá ser identificada de tal forma que puedan ser entendidos claramente de acuerdo a su función.

3.2.4 La siguiente información de contadores deberá ser comunicada desde la máquina de azar y almacenada en el sistema en unidades iguales a la denominación de la máquina de azar:

1. Total in.
2. Total out.
3. Billetes entrantes.
4. Ticket in – valor.
5. Ticket in – cantidad.
6. Ticket out – valor.
7. Ticket out – cantidad.
8. Transferencia de Ingreso de la Cuenta Sin Dinero en Efectivo.
9. Transferencia de Egreso de la Cuenta Sin Dinero en Efectivo.
10. Premios grandes pagados manualmente por el personal de juego.
11. Créditos cobrados por el jugador pagados por el personal de juego.
12. Premios grandes progresivos pagados manualmente por el personal de juego.
13. Premios progresivos pagados por la máquina de azar.
14. Ticket in promocional – valor.
15. Ticket in promocional – cantidad.
16. Ticket out promocional – valor.
17. Ticket out promocional – cantidad.
18. Promoción Electrónica Ingresada No Cobrable.
19. Promoción Electrónica Entregada No Cobrable.
20. Apuestas con Créditos Promocionales No Cobrables.
21. Derogado[1].
22. Derogado[2].
23. Juegos jugados.

NOTA: Por favor refiérase al estándar para Máquinas de Azar relativo a los contadores que debe mantener la máquina de azar. Los contadores electrónicos deberán ser comunicados directamente desde la máquina de azar al SMC, sin embargo, será aceptable la utilización de cálculos secundarios en el SMC cuando sea apropiado.

3.2.5 Un elemento de interfaz no deberá permitir que un usuario sin las autorizaciones correspondientes pueda causar la pérdida de información almacenada en los contadores.

3.2.6 El sistema debe almacenar suficiente información de medición en todo momento, es decir, el sistema debe permitir recuperar los últimos medidores o contadores válidos conocidos, mediante chequeos comprensivos de la memoria crítica del elemento de interfaz durante cada reanudación de energía 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 debe ser chequeada.
b) La memoria crítica del elemento de interfaz debe monitorearse continuamente de manera automática para detectar daño o realizar verificaciones al inicio de cada juego.

[1] Mediante Resolución Exenta N°219, de fecha 1 de abril de 2019, de la Superintendencia de Casinos de Juego.
[2] *Ídem*

c) Además, el programa de control (software que opera las funciones del elemento de interfaz) debe permitir que el elemento de interfaz asegure la integridad de todos los componentes del programa de control alojados en la memoria no-volátil.

3.2.7 El sistema debe ser capaz de almacenar medidores o contadores de al menos ocho (8) dígitos enteros de tamaño, independiente de la cantidad de dígitos decimales que puedan contemplar.

3.2.8 El SMC no deberá permitir la alteración de ninguna información de los contadores o del registro de eventos significativos, considerando, entre otros, los señalados en los estándares de máquinas de azar, que hayan sido apropiadamente comunicados desde la máquina de azar, debiendo tener controles de acceso supervisados y registros de auditoria. El registro de auditoria debe ser capaz de almacenar:

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).

Cabe señalar que estos registros de auditoria no deben ser susceptibles de ser alterados o borrados por algún usuario, sea o no autorizado.

3.2.9 El SMC debe informar o registrar todas las instancias en las que no reciba valores de contadores al final de la jornada del casino, de manera que se pueda investigar dichas circunstancias e ingresar o modificar manualmente los valores de los medidores.

3.2.10 El Sistema de Monitoreo y Control en Línea debe permitir la modificación manual de datos en los ingresos diarios cuando hayan ocurrido las siguientes circunstancias excepcionales durante el día:

a) Un borrado o “reset” de datos críticos contenidos en la memoria RAM (random Access memory o memoria de acceso aleatorio) en una máquina de azar,
b) Un “rollover” de contadores en una máquina de azar.

3.2.11 El SMC debe ser capaz de recuperar y procesar correctamente los datos de una máquina de azar que haya estado fuera de línea cuando se re-establezca la comunicación.

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 significativos hasta el momento en que pueda comunicarla al SMC. El funcionamiento de la máquina de azar podrá continuar hasta que los datos críticos puedan ser sobre escritos y perdidos, en el caso que el elemento de interfaz haya completado su capacidad. Debe existir un método para comprobar si existe corrupción de dichas ubicaciones de alojamiento de datos.

3.3 Requerimientos de comunicaciones de datos.

3.3.1 Todas las comunicaciones se deben efectuar mediante un esquema basado en un protocolo bidireccional adecuado y estándar de la industria.

3.3.2 Todas las comunicaciones de datos críticos serán basadas en el protocolo y se deberá contemplar un esquema para la detección y corrección de errores y para asegurar una precisión al nivel de noventa y nueve por ciento (99%) o más, de todos los mensajes recibidos.

3.3.3 Toda comunicación de datos críticos que pueda afectar los ingresos y que se encuentren desasegurados, 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. Es permitido que se utilice un protocolo propietario de comunicación siempre que dicha comunicación sea autentificada y validada su integridad.

3.4 Informes de excepción.

3.4.1 El SMC debe poseer la capacidad de informar y almacenar la totalidad de los eventos significativos informados por todas las máquinas de azar.

3.4.2 Cada evento significativo debe estar asociado a un número/código único que lo identifique, y debe contener también una descripción breve del evento en idioma español o en inglés, o una combinación de ambos.

3.4.3 Los eventos significativos que se generen por un dispositivo de juego, deberán ser enviados a través del elemento de interfaz al SMC utilizando un protocolo de comunicación válido el que debe ser señalado por el laboratorio en la correspondiente certificación. Cada evento significativo deberá ser almacenado en una o más bases de datos que incluya lo siguiente:

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

3.4.4 Los siguientes eventos significativos deberán ser recolectados desde la máquina de azar y transmitidos al SMC 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 pago manual de premios grandes pagados manualmente por el personal de juego, el que no incluye montos pagados como resultado de un sistema de bonificación externo o de pagos progresivos (un premio singular que exceda el límite de ganancia configurado en la máquina de azar);
    ii. El pago manual de créditos cobrados por el jugador pagados por el personal de juego; y
    iii. El pago manual de pagos progresivo pagado manualmente por el personal de juego (según el premio grande mencionado anteriormente en el literal i);
c) Apertura de puertas, de cualquier puerta que permita el acceso a un área crítica de la máquina de azar. Se pueden utilizar conmutadores de puerta (ingresos distinguibles al elemento de interfaz), a condición que su operación no resulte en mensajes redundantes o confusos;
d) Errores del verificador o validador de billetes. Los siguientes puntos “i” y “ii” deben de ser enviados como mensajes exclusivos, si es apoyado por el protocolo de comunicación:
    i. Caja de almacenamiento o stacker lleno; y

ii. Billete atascado;
e) Error de la batería de RAM en la máquina de azar, por baja carga;
f) Errores de rodillos giratorios (si es aplicable, el número específico del rodillo deberá identificarse en el código de error);
g) Errores de impresora (en caso de que la máquina utilice una impresora):
   i. Impresora vacía o poco papel; e
   ii. Impresora desconectada/fallo.

3.4.5 Los siguientes eventos significativos deben ser transmitidos al SMC y deberá existir un mecanismo para la notificación puntual. Es permitido que los siguientes eventos significativos sean enviados al sistema como un código de error genérico, en los casos que la máquina de azar no pueda distinguir los detalles del evento:

i. Pérdida de comunicación con el elemento de interfaz.
ii. Pérdida de comunicación con la máquina de azar.
iii. Corrupción en la memoria del elemento de interfaz (si está almacenando información crítica).
iv. Borrado de memoria RAM (RAM clear) y/o corrupción de la memoria RAM, con los datos críticos, de la máquina de azar, y
v. El restablecimiento de las comunicaciones.

3.4.6 El SMC debe informar toda falla de chequeo de firmas electrónicas, si se cuenta con esta facilidad.

3.4.7 Cuando sea compatible, el SMC podrá proveer una funcionalidad redundante para verificar el software del juego de la máquina de azar. Con todo, la siguiente información deberá ser verificada para su validez, previamente a la implementación:

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

3.4.8 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. Deberán existir 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.

3.4.9 En caso de un evento de fallo catastrófico, cuando el SMC no se pueda reiniciar de ninguna otra manera, deberá ser posible restablecer el sistema a partir del último punto viable de la copia de respaldo y recuperar la totalidad de los contenidos de la copia de respaldo. En esta situación se deberá considerar al menos la siguiente información:

a) Eventos significativos;
b) Información de los contadores;
c) Información de auditoria;
d) Información específica a la sala de juego, tal como el archivo de las máquinas de azar, archivos de empleados, configuraciones progresivas, etc.
e) Si se contempla la emisión de tickets, toda información utilizada en el proceso de cobro o canje de tickets incluyendo la información específica al cobro o canje de tickets fuera de línea, si corresponde.

3.4.10 Un SMC proporcionará un programa de interrogación que permita una búsqueda comprensiva en línea del registro de los eventos significativos en el presente. El programa de interrogación tendrá la habilidad de realizar una búsqueda basada en, a lo menos, lo siguiente:

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

El SMC deberá proporcionar los datos archivados o la restauración de la copia de respaldo (backup).

3.4.11 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) Sello cronometrado (en inglés time stamping) de los eventos significativos;
b) Reloj de referencia para informes; y
c) Sello cronometrado (en inglés time stamping) de los cambios de configuración.

3.4.12 Todo informe de excepción debe estar fechado con la hora local.

3.5 Requerimientos de informes.

3.5.1 El SMC debe proveer la capacidad de calcular ingresos basado en lecturas de los medidores o contadores de software recolectados en los diferentes nodos del sistema.

3.5.2 Derogado[3].

3.5.3 La información de eventos significativos y de contadores será almacenada en el SMC en una base de datos, como también los informes de los contadores generados por medio de una búsqueda sobre la información almacenada. El SMC debe tener la capacidad de generar un informe para eventos específicos en todo el sistema, para una duración y/o nodos específicos.

3.5.4 El SMC debe proveer la capacidad para que todos los informes puedan imprimirse/visualizarse para un rango dado de fechas, selección de datos pertinentes, orden de clasificación requerido y una opción para informar los datos en formato resumido o detallado.

3.5.5 Se deben considerar como mínimo los siguientes informes o reportes:

a) Reporte de las principales variables para el cálculo de los Ingresos Brutos de Juegos o Win para cada máquina de azar. Este informe deberá contener al menos el detalle diario por máquina de azar de las siguientes variables:

i. Efectivo.
ii. Ticket in (o Tarjeta in).
iii. Ticket out (o Tarjeta out).
iv. Pago manual por sistema Juego Base.
v. Pago manual por sistema Progresivo.

b) Reporte de las principales variables para el cálculo de los Ingresos Brutos de Juego o Win para el total de máquinas de azar del casino. Este informe deberá contener al menos el detalle diario para el total de máquinas de azar de las siguientes variables:

[3] Mediante Resolución Exenta N°219, de fecha 1 de abril de 2019, de la Superintendencia de Casinos de Juego.

i. Efectivo.
ii. Ticket in (o Tarjeta in).
iii. Ticket out (o Tarjeta out).
iv. Pago manual por sistema Juego Base.
v. Pago manual por sistema Progresivo.

c) Derogado[4].

d) Reporte de eventos en la máquina de azar.

e) Reporte de contadores por cada máquina de azar, considerando al menos los señalados en el numeral 3.2.4.

f) Reporte de comparación de caídas por cada medio desviado a la caja de almacenamiento o stacker (por ejemplo, billetes, tickets), con las variaciones del valor monetario y el porcentaje por cada medio y el acumulado por cada tipo.

g) Reporte de comparación entre lo que fue contabilizado como premios grandes y el valor real, con las variaciones del valor monetario y el porcentaje por cada premio grande y el acumulado.

h) Reporte de comparación entre la retención teórica y la retención real con sus variaciones.

i) Reporte de eventos significativos para cada máquina de azar.

NOTA: Es aceptable que los datos en los reportes se combinen, utilizando operaciones matemáticas, cuando sea apropiado (por ejemplo: ingresos brutos de juego, comparación teórica/real)

Los reportes antes señalados (salvo los indicados en los literales a) y b)) deberán considerar, al menos, períodos mensuales, sin perjuicio de que el sistema entregue estos reportes con una periodicidad mayor o menor al período mensual.

Los reportes deberán estar siempre a disposición de la Superintendencia de Casinos de Juego (SCJ). Las sociedades operadoras deberán tener en consideración la equivalencia de las variables utilizadas en el sistema de información operacional que esta Superintendencia requiere a los casinos de Juego (Anexo N° 1), según lo establecido en la Circular N° 34, de 14 de febrero de 2013, de esta Superintendencia o aquella que la sustituya, adicione, desarrolle y/o complemente.

3.5.6 El SMC deberá efectuar chequeos de validación para los rangos de parámetros ingresados por el usuario. Se recomienda que exista la opción de mostrar el rango válido de parámetros para cualquier campo ingresado por el usuario.

3.5.7 Todos los informes deben manejar el rango máximo de campos. Cuando el informe sea insuficiente para desplegar la información, se debe proveer una forma separada de acceder a estos datos.

[4] Mediante Resolución Exenta N°52, de fecha 20 de marzo de 2015, de la Superintendencia de Casinos de Juego.

3.5.8 Un informe vacío, es decir, un informe válido sin datos, debe cumplir con los mismos requerimientos de identificación.

3.5.9 Los informes de datos para un campo dado deben ser consistentes en todos los informes. Además, la representación de campos debe cumplir con la representación local de campos estándares similares, tales como divisas (en pesos chilenos), fecha y hora.

3.5.10 El sistema debe proveer la capacidad de generar “Resúmenes Informativos de Ingresos” tan pronto como finalice la jornada. También deberá disponer de la capacidad para generar un “Informe de Ajustes”. Este último reporte deberá contener el dato original, el dato ajustado, la fecha de cambio y la identificación del usuario que realizó el cambio.

3.5.11 El sistema debe ser diseñado de tal forma que la generación de cualquier informe no afecte la continuidad operacional del SMC frente a las máquinas de azar, para lo cual por ejemplo puede incluir el uso de una base de datos espejo, siempre que cuente con los mismos mecanismos de seguridad.

NOTA: Se entenderá por nodo a cada máquina de azar, módulo o componente del SMC o enlazado a él, que reciba y/o trasmita información al SMC.

3.6 Requerimientos del sistema computacional.

3.6.1 La arquitectura del SMC se diseñará de tal forma que bajo condiciones normales de operación no exista ninguna falla puntual que cause la interrupción de la operación normal del SMC.

3.6.2 El SMC deberá soportar una estructura jerárquica de cargos donde el nombre del usuario y la contraseña definirán el acceso a los programas o a las opciones en particular de menú o bien admitirá la entrada de acceso (en inglés login) a programas y dispositivos, basándose estrictamente en el nombre del usuario y/o número personal de identificación (PIN) y contraseña. Además, el SMC no permitirá ninguna alteración del registro de información significativa que haya sido comunicada desde la máquina de azar.

3.6.3 El SMC deberá contemplar un mecanismo para notificar al administrador del sistema y para el bloqueo de usuarios o dejar un rastro de entrada auditoria, cuando ocurra un número determinado de intentos de entradas de acceso fallidos.

3.6.4 Las bases de datos del SMC y aquellas que contengan información de contadores y de jugadores o clientes, deben ser administradas de acuerdo a las mejores prácticas de seguridad de bases de datos. Para lo anterior la sociedad operadora deberá considerar controles de acceso físico y lógico a la base de datos.

3.6.5 El SMC deberá incorporar un método seguro para evitar la modificación y visualización no autorizadas de todos los datos seguros asociados a la información crítica y de jugadores.

3.6.6 El SMC deberá estar diseñado de tal forma que los privilegios de acceso requeridos para ejecutar distintos tipos de funciones de usuario estén asociados a diferentes tipos de cuentas de usuarios, para restringir así el acceso a secciones seguras y delicadas del SMC.

3.6.7 El SMC se mantendrá en un ambiente que posea la capacidad automática de monitorear, registrar y notificar accesos por parte de cualquier persona a archivos y tablas de base de datos que contengan información segura y crítica.

3.6.8 Las descargas o cargas de código y configuraciones desde y hacia los servidores del SMC deben ser seguras, usando las mejores prácticas del sector (por ejemplo los protocolos tales como TFTP, “trivial file transfer protocol” o protocolo de transmisión de archivos muy simple, no son adecuados).

3.6.9 Todas las claves de acceso del sistema deben almacenarse en forma encriptada, no reversible.

3.6.10 Todos los intentos de accesos no autorizados deben quedar registrados en una pista de auditoria en el SMC.

3.6.11 Los sistemas usados para desarrollo o pruebas deben estar completamente separados del sistema de producción y de su base de datos.

3.6.12 Debe haber un programa disponible para emitir una lista de todos los usuarios registrados en el sistema, considerando sus niveles de privilegios.

3.6.13 En el caso que los procedimientos de acceso remoto sean aprobados por la SCJ, el SMC podrá utilizar acceso remoto controlado por contraseña para lograr el acceso al SMC a condición que se cumplan los siguientes requisitos:

a) Se deberá mantener un registro de actividad de acceso remoto de usuarios, que describa el nombre de entrada de acceso (en inglés login) del usuario, la fecha y hora, duración y la actividad desarrollada durante el acceso;
b) Los usuarios remotos no podrán realizar funcionalidades administrativas sin autorización expresa del casino de juego (por ejemplo, agregando usuarios, cambiando permisos, etc.);
c) No se permitirá el acceso sin autorización a la base de datos, a excepción de la información obtenida utilizando las funciones existentes.
d) No se permitirá el acceso sin autorización al sistema operativo; y
e) Si el acceso remoto es permanente, entonces se deberá instalar un filtro de red (firewall) para prevenir el acceso no autorizado.

3.7 Verificación del sistema.

3.7.1 El SMC deberá tener la capacidad de verificar la identidad de todas las máquinas de azar antes de que se alisten en el sistema, como también en todo momento en que se vuelvan a alistar en el sistema después de que una comunicación entre ellos y el SMC se pierda, y luego se restaure.

3.7.2 El SMC podrá tener la capacidad de ejecutar la verificación de firmas electrónicas en el software que opera en la máquina de azar, usando el proceso de verificación manejado por el protocolo utilizado para la comunicación entre la máquina de azar y la interfaz inmediata de comunicación de la máquina.

3.7.3 Los componentes/módulos del software del SMC serán verificables por un método seguro a nivel del sistema, denotando el número/código de identificación del programa y versión. El SMC deberá tener la capacidad de permitir una verificación de integridad de los componentes/módulos de manera independiente, por medio de un método externo, el que será requerido para todos los programas de control que puedan afectar la integridad del mismo. 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.

3.7.4 El SMC deberá tener la capacidad de autenticar periódicamente los distintos nodos del sistema, y al menos una vez por día.

3.7.5 Derogado[5].

3.7.6 Cuando el SMC no puede autenticar un nodo, debe excluir todas las máquinas de azar y todo otro componente del sistema enlazado con los componentes del SMC que no están autenticados. Sin embargo, el dispositivo del SMC que ha fallado continuará monitoreando y detectando todos los eventos de seguridad de todos los dispositivos enlazados con él.

3.7.7 Derogado[6].

3.7.8 El SMC deberá tener la capacidad de validar la identidad del dispositivo desde el cual provengan datos de comunicación, y de rechazar paquetes de datos recibidos desde cualquier nodo no autenticado por el SMC. Toda comunicación recibida desde cualquier nodo que no haya sido autenticado por el SMC debe informarse en los informes por excepción.

3.7.9 Derogado[7].

3.7.10 Derogada[8].

3.7.11 El SMC deberá implementar un método para verificar la integridad de todo el software de aplicación instalado para manejar la funcionalidad del SMC, permitiendo la verificación de las firmas electrónicas de todos los módulos de software de aplicación del SMC, en particular las firmas de los programas que generan los informes relevantes señalados en el numeral 3.5.5, mediante métodos externos de validación que comparen los valores calculados de firmas con aquellas almacenadas en los medios externos de verificación.

3.8 Requerimientos de conexión con otros sistemas.

3.8.1 La conexión con todos los otros sistemas debe ser mediante un protocolo de comunicación adecuado y bidireccional.

3.8.2 Los sistemas auxiliares al SMC solo deberán tener permisos de lectura y no deberán tener capacidad alguna de modificar valores del SMC, salvo que se le otorguen los permisos necesarios y se utilice un protocolo de comunicación válido.

3.8.3 El protocolo de conexión debe ser capaz de manejar informes de eventos significativos de los sistemas auxiliares. Como mínimo, el SMC debe ser capaz de detectar e informar cuando la comunicación normal con el sistema auxiliar se haya perdido y restaurado.

3.8.4 Será permitido que los sistemas auxiliares ingresen información adicional al SMC, pero nunca podrán modificar datos comunicados por las máquinas de azar.

[5] Mediante Resolución Exenta N°219, de fecha 1 de abril de 2019, de la Superintendencia de Casinos de Juego.
[6] *Ídem*
[7] *Ídem*
[8] *Ídem*

3.8.5 Solo sistemas autorizados por la SCJ podrán copiar información de jugadores o clientes y/o de configuraciones de las máquinas de azar. Será permitido extraer la información de contadores (mediante un proceso de solo lectura) a sistemas propios del casino para efecto de análisis de negocio.

3.8.6 Entre los sistemas auxiliares existentes se señalan:
a) Sistema TITO
b) Sistemas de progresivos
c) Sistemas cliente/servidor
d) Sistemas de interfaces de jugador

3.9 Requisitos de los elementos de interfaz

3.9.1 Cada máquina de azar instalada en una sala de juego deberá tener un dispositivo o facilidad (es decir, un elemento de interfaz) instalado dentro de la máquina de azar en un área segura, que proporcione la comunicación entre la máquina de azar y un colector de datos externo. Las medidas de seguridad de la ubicación del elemento de interfaz o puerto de comunicaciones se encuentran descritas en el estándar de Máquinas de azar.

En el caso que no sea posible que estos dispositivos sean ubicados dentro de la máquina de azar o que existan concentradores de los mismos (switch u otros), éstos no podrán ser accesibles al público y deberán contar con medidas adecuadas de seguridad.

3.9.2 Si los contadores de las máquinas de azar no se están comunicando directamente al SMC, el elemento de interfaz deberá mantener contadores electrónicos separados, de longitud suficiente para prevenir la pérdida de información de los contadores cuando se reinicien a cero (0) (en inglés roll-over) o disponer de un medio para poder identificar múltiples reinicios a cero (0) según lo dispuesto en las máquinas de azar conectadas. Estos contadores electrónicos deben ser capaces de ser mostrados según requerimiento, a nivel del elemento de interfaz a través de un método de acceso autorizado.

3.9.3 El elemento de interfaz deberá retener la información requerida después de una pérdida de energía eléctrica hasta que los datos sean enviados en forma segura al SMC. Si estos datos son almacenados en la memoria de acceso aleatoria RAM volátil, dentro del elemento de interfaz se deberá instalar una batería de respaldo.

3.10 Requisitos del procesador frontal y el colector de datos.

3.10.1 Un SMC podrá poseer un procesador frontal (en inglés 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, recolectarán todos los datos de las máquinas de azar conectadas. La comunicación entre los componentes debe ser a través de un método válido y por lo menos deben cumplir con los requisitos de protocolos de comunicación estipulados en este documento. Si el procesador frontal mantiene información en memoria intermedia (en inglés buffered) o en un diario, entonces deberá existir un medio para prevenir la pérdida de información crítica contenida.

3.11 Requisitos de la estación de trabajo.

3.11.1 Un Sistema SMC debe tener una aplicación o la habilidad de capturar y procesar todos los mensajes de pagos manuales de cada máquina de azar. Los mensajes de pagos manuales deberán crearse para las ganancias individuales de premios grandes del juego base, premios grandes progresivos y pagos de créditos acumulados (créditos cobrados por el jugador), que resulten en pagos manuales.

3.11.2 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 azar;
e) Denominación;
f) Las cantidades del premio grande del juego base, premios grande progresivo y crédito acumulado o cobrado por el jugador;
g) La cantidad para el jugador;
h) El total de créditos jugados y el resultado del juego que entregó el premio;
i) Las lecturas de los contadores electrónicos; y
j) Firmas de verificación (huellas).

3.11.3 Un SMC deberá tener una aplicación o la habilidad de permitir accesos controlados a toda la información de operación y será capaz de generar al menos, todos los informes mandatarios especificados en este documento.

3.11.4 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 inglés 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, estos sistemas podrán ser ensayados, para el control de su correcto funcionamiento y de su versión, si es solicitado y, cuando se trate de una facción integrada en un SMC).

3.12 Facciones adicionales del sistema

3.12.1 Si es compatible, un SMC podrá utilizar tecnología Flash para instalar el software del elemento de la interfaz, a condición que cumpla con todos los requisitos que se indican 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 momento en el sistema sin la intervención del usuario.
b) Un registro de auditoria debe registrar la hora y fecha de una descarga Flash y alguna provisión deberá efectuarse para asociar este registro con la versión o versiones del código que fue descargado y el usuario que inició la descarga. Deberá emitirse un reporte separado del registro de auditoria de descarga Flash.
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 que posea 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 en las salas de juego. Adicionalmente, todos los archivos Flash deberán estar disponibles para poder verificar las referidas firmas.

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

ANEXO N°1, TABLA DE EQUIVALENCIA ENTRE LOS CONTADORES DE LAS MÁQUINAS DE AZAR Y LAS VARIABLES UTILIZADAS EN EL SISTEMA DE INFORMACIÓN OPERACIONAL DE CASINOS DE JUEGO.

TABLA DE EQUIVALENCIAS

N°	NOMBRE CONTADOR EN ESTANDAR SISTEMA DE MONITOREO	NOMBRE VARIABLE EN SISTEMA DE INFORMACIÓN OPERACIONAL
1	Total in	"Total jugado" o "Total in"
3	Billetes entrantes	"Efectivo"
4	Ticket in – valor	**"Ticket in** o Tarjeta in"
6	Ticket out – valor	**"Ticket out** o Tarjeta out"
8	Transferencia de Ingreso de la Cuenta Sin Dinero en Efectivo	"Ticket in o **Tarjeta in"**
9	Transferencia de Egreso de la Cuenta Sin Dinero en Efectivo	"Ticket out o **Tarjeta out"**
10	Premios grandes pagados manualmente por el personal de juego	"Premios grandes. Pago manual por sistema Juego Base"
11	Créditos cobrados por el jugador pagados por el personal de juego	"Ticket out o Tarjeta out"
12	Premios grandes progresivos pagados manualmente por el personal de juego	"Premios grandes. Pago manual por sistema Progresivo"
13	Premios progresivos pagados por la máquina de azar	Incluido en "Ticket out o Tarjeta out"
14	Ticket in promocional – valor	**"Ticket in promocional** o Tarjeta in promocional"
16	Ticket out promocional – valor	**"Ticket out promocional** o Tarjeta out promocional"
18	Promoción Electrónica Ingresada No Cobrable	"Ticket in promocional o **Tarjeta in promocional"**
19	Promoción Electrónica Entregada No Cobrable	"Ticket out promocional o **Tarjeta out promocional"**
23	Juegos jugados	"Número de jugadas"
	Identificador único de máquina de azar (1)	"Código Casino máquina de azar"
	"Valor actual" (3) "Valor o monto actual de pozo para cada progresivo" (4)	"Pozo Total Inicial por día"
	Informe de tickets expirados (2)	"Tickets expirados (monto)"
	Informe de tickets expirados (2)	"Número Tickets expirados"

(1) Variable definida en "Estándar para Sistemas de Monitoreo y Control en Línea"
(2) Informe requerido en "Estándar para Sistemas de Tickets Entrantes /Salientes (TITO)"
(3) Variable para progresivo individual definida en "Estándares para Máquinas de Azar"
(4) Variable definida en "Estándar para Sistemas Progresivos"