SCJ | SUPERINTENDENCIA DE CASINOS DE JUEGO

CIRCULAR Nº 049

SANTIAGO, 13 FEB 2014

VISTOS

Lo dispuesto en los artículos 1, 2, 36, 37 N° 2 y 42 N° 9 de la Ley N° 19.995; y atendido lo prescrito en los artículos 3 letra j) y 6 del mismo cuerpo legal, en el artículo 33 y 34 del Decreto Supremo N° 287, de 2005, del Ministerio de Hacienda, que aprueba el Reglamento de Funcionamiento y Fiscalización de Casinos de Juego; el Decreto Supremo N° 547, de 2005, del Ministerio de Hacienda, que aprueba el Reglamento de Juegos de Azar en Casinos de Juego y Sistema de Homologación; la Resolución Exenta N° 157, de fecha 10 de julio de 2006, y sus modificaciones, que aprueba el "Catálogo de Juegos que podrán desarrollarse en los casinos de juego", en adelante "Catálogo de Juegos", y en uso de las facultades legales, en especial, aquélla contemplada en el artículo 42 N°7 del referido cuerpo legal, en el Decreto Supremo N° 573, de 2012, del Ministerio de Hacienda; así como en las demás disposiciones pertinentes; y

CONSIDERANDO

1. Que, el artículo 1 de la ley N° 19.995, señala que "*la autorización, funcionamiento, administración y fiscalización de los casinos de juego, así como los juegos de azar que en ellos se desarrollen, se regularán por las disposiciones de la presente ley y sus reglamentos*".

2. Que, por su parte, el inciso 1 del artículo 2 de la ley N° 19.995, señala que "*corresponde al Estado determinar, en los términos previstos en esta ley, los requisitos y condiciones bajo los cuales los juegos de azar y sus apuestas asociadas pueden ser autorizados, la reglamentación general de los mismos, como también la autorización y fiscalización de las entidades facultadas para desarrollarlos, todo lo anterior, atendido el carácter excepcional de su explotación comercial, en razón de las consideraciones de orden público y seguridad nacional que su autorización implica...*"

3. Que el artículo 6° de la Ley N° 19.995 establece que "...Los operadores sólo podrán utilizar las máquinas e implementos de juegos de azar que se encuentren previamente homologados e inscritos en el registro que al efecto llevará la Superintendencia". En el mismo sentido, el inciso primero del artículo 29 del Decreto Supremo N° 547, de 2005, del Ministerio de Hacienda, señala que "...*La práctica y explotación de los juegos de azar en los casinos de juego, sólo podrá efectuarse con el material de juego constituido por máquinas e implementos de juegos de azar que corresponda a los tipos y modelos previamente homologados por la Superintendencia*".

4. Que, por otro lado, el artículo 42 N° 9 de la ley N° 19.995, señala que "*corresponderá al Superintendente (...) Dictar las instrucciones técnicas, procedimientos y registros, mediante los cuales las entidades fiscalizadas deberán abrir, desarrollar y cerrar las operaciones diarias de los juegos y apuestas asociadas*".

5. Que, el artículo 26 del Decreto Supremo N° 547, de 2005, del Ministerio de Hacienda, señala que "*los operadores llevarán un registro diario de la apertura y cierre de las mesas y de las recaudaciones brutas por concepto de apuestas, por cada una de las mesas y de los juegos que se practiquen en el establecimiento, para establecer los flujos de ingresos y egresos en cada día de funcionamiento de las salas de juego, de conformidad a las instrucciones que la Superintendencia imparta al efecto y sin perjuicio de lo dispuesto en el artículo siguiente...*"

6. Que, a su vez, en conformidad al inciso 1 del artículo 6 del Decreto Supremo N° 287, de 2005, del Ministerio de Hacienda "*los casinos de juego funcionarán todos los días del año, salvo aquellos días de excepción establecidos por la ley. Cada sociedad operadora determinará el horario de funcionamiento del establecimiento, y de los juegos que se desarrollen en él. En todo caso, ningún casino de juego, cualquiera sea el día o la época del año, podrá funcionar menos de seis hora en el día*". (El subrayado es nuestro).

7. Que, en ese contexto normativo, corresponde a esta Superintendencia dictar las especificaciones técnicas que deberán cumplir las sociedades operadoras necesarias para asegurar la correcta operación y disponibilidad de las máquinas de azar, como los demás implementos que inciden en el normal desarrollo de los mismos, entre los cuales están los sistemas informáticos y sistemas de video vigilancia que podrán ser utilizados por las sociedades operadoras en la práctica y explotación de los juegos de azar en sus casinos de juego, estableciendo un estándar para las condiciones de mantención de los referidos sistemas y las condiciones ambientales requeridas para su correcta operación, que permitan disminuir las probabilidades de eventos de falla y asegurar la continuidad operativa de los juegos de los juegos de azar.

8. Que, las referidas especificaciones técnicas se dictan con el objeto de garantizar la integridad, disponibilidad y confiabilidad de la información residente y circulante en los casinos de juego, relacionada con datos sensibles de clientes, recaudaciones por concepto de apuestas, operación de los juegos de azar, estadísticas y toda aquella información relevante para esta Superintendencia necesaria para preservar la fe pública. Lo anterior, ante la eventualidad de catástrofes, atentados, acciones maliciosas, fallas técnicas, falla de proveedores, cortes eléctricos, etc.

9. Que por lo expuesto y en virtud de las normas vigentes,

IMPÁRTENSE las siguientes:

INSTRUCCIONES GENERALES ACERCA DE CONDICIONES MINIMAS DE ARQUITECTURA DE HARDWARE, SOFTWARE Y COMUNICACIONES, SOBRE LA QUE SE INSTALAN Y COMUNICAN LOS SISTEMAS QUE CONTROLAN EL JUEGO Y LO SUPERVISAN EN CASINOS DE JUEGO AUTORIZADOS AL AMPARO DE LA LEY N°19.995

Para efectos de la presente Circular se deben considerar las siguientes definiciones:

1. Definiciones previas

1.1 Alta Disponibilidad: Es la capacidad de mantener activo un servicio cualquiera, durante un tiempo determinado, después de producirse una falla en éste.

1.1.1 Activo – Activo: Configuración de alta disponibilidad en la que todos sus miembros se encuentran permanentemente prestando servicios y en la que se distribuye la carga de trabajo.

1.1.2 Activo – Pasivo: Configuración de alta disponibilidad en la que uno de sus miembros se encuentre activo y asumiendo toda la carga de trabajo, los demás nodos permanecen inactivos y asumen carga de trabajo cuando el primer nodo sufre alguna caída.

1.2 Redundancia: Se refiere a la replicación de componentes, nodos o equipamiento completo, así como caminos u otros elementos de la red y que su función principal es ser utilizados en caso de la caída de un equipo o sistema.

1.3 Data Center: Toda aquella ubicación donde se concentran los recursos de información de la organización.

1.4 Switch de Distribución: Se refiere al equipamiento de comunicaciones conectado directamente a las máquinas de azar.

1.5 Planes de Recuperación de Desastres o DRP: Conjunto documentado de tareas y procesos orientados a recuperar las operaciones tecnológicas de un casino, ante la ocurrencia de un desastre, o fallas importantes.

2. Requerimientos Mínimos DATA CENTER

Se requiere que cada casino de juego cuente con al menos un Data Center, en el que se aloje la infraestructura, con especial énfasis en los servidores destinados a juegos de azar, equipamiento de comunicaciones y seguridad, y sistemas de Circuito Cerrado de Televisión, en adelante "CCTV", de los casinos de juego.

Para cumplir este objetivo, se requiere que las sociedades operadoras cumplan con los siguientes requerimientos mínimos, en los términos que se señalan a continuación:

2.1 DATA CENTER

2.1.1 Obra Gruesa.

La sala en que se aloje la infraestructura de la Tecnología de la Información, en adelante "TI", (Data Center), deberá contar con las siguientes características mínimas de construcción:

I. Deberá estar construida con materiales sólidos tales como: hormigón, ladrillo y elementos estructurales de acero, que pueden incluir recubrimientos, éstos últimos deben ser resistente al fuego por a lo menos

30 minutos, pudiendo complementarse con el uso de pinturas que deben ser intumescentes o ignífugas.

II. Deberá contar con aislación que impida la filtración de agua, además de disminuir las posibles consecuencias provocadas por otras amenazas ambientales para el equipamiento, como terremotos, explosiones, o daños causados por personas.

III. El Data Center podrá contar en uno de sus muros laterales con una superficie translúcida o transparente no removible y resistente a impactos y de la misma forma resistente al fuego por a lo menos 30 minutos, sólo si ésta colinda directamente con el espacio físico que ocupa el área de TI, lo anterior con el fin de permitir el monitoreo visual del funcionamiento del equipamiento y condiciones ambientales por parte de los trabajadores del área.

IV. El Data Center deberá contar, además, con puertas sólidas e ignífugas por al menos 30 minutos.

V. La sociedad operadora deberá contar con todas las certificaciones de los fabricantes de los materiales que conforman el Data Center, que permitan determinar que los materiales utilizados cumplen con los presentes requisitos mínimos.

2.1.2 Control de Acceso.

I. Las sociedades operadoras deberán implementar un sistema de control de acceso que permita restringir y auditar los ingresos y salidas al Data Center. Asimismo, las sociedades operadoras deberán implementar un procedimiento de acceso y registro de actividades en el Data Center, en el que se deberá registrar la identificación de la persona, los respectivos horarios de entrada y salida, además de las actividades realizadas por quien ha solicitado el acceso, tanto para personal interno como externo.

II. El Data Center, deberá contar con equipamiento de video vigilancia, con sistema de grabación, en modalidad 24X7 y/o con detección de movimiento, que permita registrar las actividades realizadas por cualquier persona en su interior, así como en los puntos de acceso, debiendo considerarse una retención de 15 días para situaciones normales y de 3 meses, en caso de producirse anomalías al interior del Data Center como fallas de sistemas que produzcan discontinuidad en la operación del casino de juego o intrusiones y otras que el casino determine.

2.1.3 Protección del Cableado al Interior del Data Center.

I. Con la finalidad de impedir o dificultar el acceso no autorizado o accidental al cableado al interior del Data Center, las sociedades operadoras deberán instalar un piso técnico sobre la escalerilla o cualquier otro método que permita aislar en forma ordenada las redes eléctricas y de datos, y dirigirlas hacia los diferentes racks del Data Center, cuando ésta haya sido ubicada en el suelo, o cielo falso, cuando se haya instalado pegada a la losa superior y en caso de encontrarse dichas escalerillas a menos de 2,5 metros.

II. El cableado de datos, eléctrico, de CCTV u otro que se haya instalado al interior del Data Center deberá ser canalizado usando escalerillas

metálicas u otro método de igual o mejor eficacia, debiendo encontrarse separado de acuerdo a su uso o naturaleza.

2.1.4 Climatización.

I. Todo Data Center, deberá contar con equipamiento de climatización redundante.

II. En este contexto, al menos un equipo de climatización deberá ser de tipo misión crítica, con alto grado de confiabilidad y eficiencia, capaz de controlar además de la temperatura, la humedad existente en su interior y deberá contar con la capacidad necesaria para soportar todo el equipamiento instalado al interior del Data Center. Cabe señalar que al referido equipamiento también se le denomina sistema de climatización precisa.

III. Por otro lado, el o los equipos secundarios, necesarios para completar la mencionada redundancia, podrán ser de tipo Split u otro, siempre que permita mantener la continuidad operacional del Data Center de forma de no interrumpir los servicios que éste presta al casino de juego.

2.1.5 Respaldo de Energía.

I. El Data Center deberá contar con al menos un Sistema de Alimentación Ininterrumpida, en adelante "UPS", que permita autonomía del equipamiento por un periodo de al menos 20 minutos. Este sistema deberá ser configurado para realizar la conmutación automática en caso de caída del suministro principal de energía y su respectiva vuelta atrás.

II. De la misma forma, las sociedades operadoras deberán contar con al menos una UPS que mantenga en operación las máquinas de azar instaladas en la sala de juegos o al menos su Unidad de Proceso Central, en adelante "CPU", esto con el fin de no perder información cuando exista corte de energía, permitiendo que dicha información pueda ser enviada a los sistemas principales una vez que se recupere el suministro eléctrico.

III. Todos los sistemas UPS del casino de juego, ya sea para el o los Data Center como para los restantes dispositivos y máquinas de azar, deberán, a su vez, estar respaldados por un sistema de generación de energía.

2.1.6 Detección y Extinción de Incendios.

I. El Data Center deberá contar con un sistema automático de detección de incendios el que deberá alertar mediante señales audibles y visibles, la existencia de fuego al interior del mismo.

II. Las sociedades operadoras deberán contar con un sistema automático o manual para el control de incendios mediante sistema extintor, no conductor, capaz de controlar fuegos de tipo A (madera, papel, trapo, etc.), B (gasolinas, pinturas, etc.) y C (equipos eléctricos conectados). En caso de optar por un sistema de extinción manual se deberá implementar un procedimiento particular para el control de incendios en el Data Center, el que deberá estar visible a quienes corresponda y justo en el acceso

principal a éste. En caso de considerar un sistema control de incendio mediante extintores manuales, el casino deberá contar con turnos de 24 horas para esta finalidad.

2.1.7 Control de Temperatura y Monitoreo.

El Data Center deberá contar con un sistema electrónico de control de temperatura, que permita monitorear permanentemente y de manera remota la existencia de variaciones en su interior, alertando de manera automática al operador o funcionario correspondiente.

2.1.8 Condiciones Generales del Data Center.

El o los Data Center, se deberá(n) mantener limpio(s) y ordenados, sin elementos ajenos a la operación de éste, como equipamiento en mal estado o fuera de los respectivos racks.

2.1.9 Equipamiento fuera del Data Center.

I. Todo equipamiento destinado a soportar infraestructura tecnológica, comunicaciones y otras funciones tecnológicas, que se encuentre fuera del Data Center, deberá contar con condiciones de seguridad que impidan el acceso y manipulación de éste por parte de clientes, personas externas a la operación del casino y personal del casino no autorizado, es decir, en salas o gabinetes con acceso restringido, mediante cualquier sistema de control de acceso, que incluye la opción de llaves y cerraduras tradicionales.

II. Asimismo, las sociedades operadoras deberán contar con equipamiento en condiciones ambientales mínimas para su correcta operación, cuidando de mantener las condiciones de temperatura necesarias para la adecuada operación de equipos electrónicos.

2.2 Sistemas.

Las sociedades operadoras deberán implementar los siguientes requerimientos mínimos respecto de los sistemas y servidores.

I. Los sistemas y servidores que en caso de fallas impidan la continuidad operacional del casino de juego, o que se encuentren directamente asociados a la operación de los juegos de azar, deberán estar implementados en una configuración en alta disponibilidad, pudiendo ser éstos físicos o virtuales, con a lo menos dos servidores en aquellos casos en que éste se encuentre instalado sobre servidores físicos. Si dichos sistemas se encontrasen instalados en una plataforma virtual, ésta deberá entregar la posibilidad de que el sistema pueda migrar entre al menos dos host de virtualización, garantizando siempre el rendimiento y disponibilidad de los señalados sistemas.

En el caso de los sistemas complementarios y no relacionados directamente a las actividades de juego la sociedad operadora, podrá contar con otros mecanismos que permitan aumentar el nivel de

disponibilidad de los servidores o sistemas, como discos, fuentes, y otros elementos internos redundantes.

II. Deberán existir diagramas o modelos en los que se describa la arquitectura de los sistemas, en sus componentes principales de hardware y software, de forma que sean auditables por esta Superintendencia. Para ello, el casino de juego deberá suministrar documentación con la descripción de la arquitectura y funcionalidad de cada sistema. Dicha documentación deberá incluir como mínimo información sobre: arquitectura de los sistemas, o modelos esquemáticos funcionales; conectividad y características de la misma; planos eléctricos y de red de datos; restricciones y requerimientos de la instalación; estabilidad; disponibilidad del sistema; tiempo medio entre fallas; tiempo medio de recuperación del sistema; tolerancia a fallas; escalabilidad y seguridad.

III. La información almacenada en las bases de datos de los sistemas relacionados al juego o complementarios para dicho propósito, así como los reportes o certificados de los mismos, no podrá ser alterada por el casino de juego, salvo que se requiera por motivos técnicos, los cuales deberán ser informados a la Superintendencia de Casinos de Juego, y mantener un registro auditable de las acciones realizadas.

IV. El o los servidores deberán estar alojados en un Data Center con las condiciones ya señaladas en la presente circular, al interior de las dependencias del propio casino de juego, que no revistan la calidad de servicios anexos del mismo.

V. La sociedad operadora deberá implementar procedimientos de control, con el objeto de asegurar que los registros horarios y de fecha de logs para todos los sistemas, sean las mismas que se despliegan en las diferentes máquinas de azar controladas o asociadas a dichos sistemas o en los distintos componentes asociados y corresponda a la hora y fecha efectiva del registro. En casos excepcionales, podrá existir una diferencia horaria entre estos sistemas, la que no podrá exceder los 5 minutos, debiendo constar su existencia en un procedimiento interno. Cabe señalar que la referida diferencia horaria deberá ser informada a esta Superintendencia, señalando su origen y los sistemas que se ven afectados.

VI. Será de exclusiva responsabilidad del fabricante, proveedor y/u operador de los sistemas que sean utilizados en los casinos de juego, dar estricto y oportuno cumplimiento a las leyes de derecho de autor, propiedad intelectual, marcas, patentes, nombres, diseños registrados u otras de esa naturaleza que sean aplicables a los referidos sistemas. Quedan liberados de toda responsabilidad derivada del incumplimiento de dicha normativa tanto esta Superintendencia, como el laboratorio certificador que eventualmente efectúe las pruebas y ensayos pertinentes.

VII. Todos los sistemas utilizados en el casino de juego, deben cumplir con normas y políticas de seguridad que permitan mantener la integridad, disponibilidad y confidencialidad tanto de los registros de auditorías y eventos, históricos y en línea, como de la información que en ellos se administra, lo que deberá ser verificable mediante la existencia de

procedimientos de seguridad aplicados por la sociedad operadora. Además, los registros e información antes señalados deberán estar disponibles para la Superintendencia cuando sea requerida su entrega o acceso.

VIII. Las sociedades operadoras no deberán permitir el acceso remoto al o los servidores de los sistemas asociados directa o indirectamente a los juegos de azar, desde una red no perteneciente a las instaladas en el casino de juego. Sólo en casos excepcionales, cuando se requiera conexión con el proveedor del sistema o para soluciones a contingencias, se permitirá el acceso desde una red externa, para lo cual el casino de juego deberá tener elaborados y aplicados procedimientos de acceso de terceros a sus sistemas, que incluyan el registro y capacidades para posibilitar auditoría del usuario que realizó el acceso y de sus acciones en el sistema. Los servidores, sus configuraciones, los elementos de red y seguridad que conformen la solución, deberán impedir todo acceso remoto a ellos, entendiendo por tal, cualquier acceso no autorizado desde fuera de la red del casino de juego.

IX. Si se requiere acceso periódico desde una red externa, respecto de las funciones de soporte o mantenimiento de los sistemas, dicha situación deberá ser formalizada de acuerdo a procedimientos de seguridad para acceso de terceros, debiendo el casino de juego poseer registros auditables de tales accesos.

X. Los servidores, que alojen los sistemas relacionados al juego, deberán estar dedicados exclusivamente a tal objeto.

XI. El o los servidores deberán poseer sistemas de seguridad lógica y física formalizados en procedimientos, sistemas de protección contra accesos no autorizados y contra la instalación o ejecución de programas potencialmente peligrosos, los que también deberán estar formalizados en procedimientos. Además, se deberá contar con una definición actualizada de los perfiles de acceso por sistema y por usuario, considerando una adecuada segregación de funciones.

XII. Las redes inalámbricas que sean utilizadas para sistemas de juego, deberán considerar, al menos, las siguientes medidas de seguridad:

a) Deberán ser seguras, verificando que solo dispositivos validados puedan acceder a la red mediante algoritmos de encriptación, los que deberán ser nuevamente autenticados en el caso de producirse desconexiones o ante cualquier señal de acceso inadecuado de los terminales de juego. Estos dispositivos deberán ser validados mediante un identificador único, ya sea por su dirección de hardware (MAC), u otro método de igual o mejor eficacia;
b) Deberán contar con un sistema de detección de intrusos basado en red, capaz de detectar intromisiones en el tráfico de la red, en forma independiente del método de autenticación o encriptación utilizado;
c) Se deberán separar de cualquier otra red del casino mediante un sistema de seguridad de cortafuegos (firewall);
d) Se deberá ocultar el nombre de la red inalámbrica;

e) Toda la comunicación entre los distintos dispositivos inalámbricos y el servidor deberá utilizar un apropiado protocolo de autenticación y encriptación, de manera tal de proveer una mutua autenticación, debiendo asegurar la integridad y confidencialidad de la información transmitida;
f) Todos los dispositivos o componentes físicos que conforman las redes inalámbricas, como por ejemplo equipos de tipo "access point" y "routers", deberán contar con una adecuada seguridad física.
g) Se deberán modificar todas las contraseñas por defecto (*default*) que incluyan los distintos dispositivos que intervienen en las redes inalámbricas;
h) Se deberá implementar un adecuado control de acceso a la administración de estas redes considerando segregación de funciones y las mejores prácticas en seguridad de la información;
i) Deberán existir registros de auditoria respecto de cualquier modificación a la red, los que deberán ser mantenidos por al menos 6 meses; y,
j) Las redes inalámbricas deberán estar debidamente documentadas, describiendo su topología, equipamiento involucrado y las áreas en las cuales estas redes se encuentran disponibles.

2.3 Respaldo y Disponibilidad de la Información.

I. Los sistemas asociados al juego directa o indirectamente deberán ser respaldados al menos diariamente, tanto en su configuración como su información, mediante procedimientos de respaldo documentados que permitan, en el caso que el sistema sufra una falla que impida su reiniciación, recuperar en forma rápida la operación del casino, con información actualizada.

II. Las sociedades operadoras deberán mantener un respaldo de todos los sistemas y datos relacionados al juego, con acceso directo para su consulta y/o restauración desde el propio Data Center por al menos 6 meses. Simultáneamente, se deberá almacenar dicha información en un repositorio externo por hasta 6 años, actualizado al menos mensualmente, bajo normas de seguridad estrictas y respaldado por niveles de servicio de un proveedor externo y/o interno, esto sin perjuicio de los plazos que establezca el Código Tributario o cualquier otro cuerpo legal o reglamentario, para los registros contables u otro tipo de información.

2.4 Redes de Datos y Enlaces.

2.4.1 Segmentación de Redes (Física o lógica).

Las redes de datos que comunican los sistemas de juego del casino con los servidores de monitoreo en línea de las máquinas de azar (SMC), deberán encontrarse física o lógicamente separadas de las redes de acceso de los usuarios, tanto a los sistemas como a Internet. Asimismo, se deberán implementar sistemas de seguridad de redes, firewall o equivalente en los puntos que por motivos de fuerza mayor el tráfico de una de estas redes sea ruteado hacia otra, aplicando filtros de tráfico entre uno y otro segmento.

2.4.2 Separación Física de Redes.

Todos los sistemas relacionados al juego, deberán encontrarse física o lógicamente separados de las redes de trabajo ubicadas en el casino de juego. En aquellos puntos en que las redes de datos deban converger por motivos técnicos o requerimientos del negocio, deberá considerarse la instalación de un sistema de seguridad de cortafuegos o equivalente entre ellas, permitiéndose una ruta de red alterna sólo para los propósitos de redundancia, la que deberá, también, pasar a través de, a lo menos, un sistema de seguridad de cortafuego o equivalente. El mecanismo de seguridad utilizado deberá mantener un registro de auditoria, con al menos las siguientes actividades:

1. Intentos de conexión con éxito y fallidas, y
2. Direcciones IP de inicio y destino, número de puerto y dirección MAC de los dispositivos.

2.4.3 Disponibilidad Equipamiento de Redes.

I. Los Switch de distribución deben contar con algún mecanismo de reemplazo u otro que asegure la continuidad de los servicios ante fallas o interrupciones.

II. Por su parte, el equipamiento que eventualmente "rutee" el tráfico desde los Switch de distribución hacia el equipamiento de servidores u otras redes, deberán contar con una configuración redundante, de alta disponibilidad.

III. En caso que el casino, cuente con servicios conjuntos con otros casinos, el equipamiento de comunicaciones, seguridad y enlaces de datos entre ellos, deberá estar configurado de forma redundante y en alta disponibilidad.

IV. La solución de reemplazo para todos los casos deberá ser de fácil reposición y configuración.

V. Con el fin de facilitar el reemplazo de un equipo de comunicaciones, el casino de juego debe disponer y aplicar un procedimiento de respaldo, que considere las configuraciones de sus equipos de comunicaciones y redes.

2.4.4 Enlaces.

Aquellos casinos que utilicen sistemas interconectados entre sí, deberán contar con enlaces de comunicaciones redundantes, que para el caso del enlace secundario o de respaldo deberá contar con velocidades de, al menos, 10Mbps nacional.

2.5 CCTV.

2.5.1 Data Center:

I. El casino deberá contar con un Data Center en el que se alojen los servidores de Video Vigilancia, pudiendo ser exclusivo para el equipamiento de Video Vigilancia o compartido con el que mantiene el equipamiento y sistemas de TI.

II. En el evento de ser un Data Center exclusivo para los servidores CCTV, éste deberá cumplir con los mismos requerimientos mínimos ya señalados en el numeral 2 del presente documento.

2.5.2 Seguridad del Equipamiento:

I. Los operadores de los sistemas de CCTV no podrán contar con perfiles, que le permitan eliminar o modificar los datos y/o grabaciones generadas por ellos, limitándose este tipo de acceso, a quienes sean declarados como administradores de dicha información por parte de la sociedad operadora, de acuerdo a sus propios criterios.

II. Las condiciones de seguridad, continuidad e integridad del equipamiento e información de los sistemas CCTV deberán cumplir con los mismos requerimientos mínimos establecidos en esta misma norma para el resto de los sistemas y datos relacionados con el juego en sus numerales 2.1 y 2.2.

2.6 Recuperación de Desastres.

Las sociedades operadoras deberán realizar la implantación de Planes de Recuperación de Desastres, para la operación de Tecnologías de información en los casinos.

2.6.1 Documentación.

El casino de juego deberá redactar y mantener actualizado un documento que explique en forma detallada los diferentes niveles y escenarios de contingencia tecnológica a que se pueden enfrentar las operaciones tecnológicas de los casinos de su administración, y los procesos y procedimientos que permitan operar en contingencia y recuperar el estado operativo de los sistemas relacionados con juegos de azar. Este documento se referenciará como DRP.

2.6.2 Pruebas del Plan.

El casino de juego deberá realizar pruebas periódicas de los planes definidos en el DRP, dejando la evidencia detallada de las pruebas realizadas y de sus resultados, los que deberán considerar la restauración de datos respaldados.

2.6.3 Notificación a la Superintendencia de Casinos de Juego.

El casino de juego deberá informar a la Superintendencia cuando el plan sea modificado, en un plazo máximo de una semana.

2.6.4 Varios.

El plan deberá considerar los procedimientos operación en contingencia y restauración de servidores físicos y virtuales, motores de bases de datos, sistemas de comunicaciones, sistemas eléctricos y equipamiento de todo tipo relacionado con los juegos de azar.

3. Vigencia

Las presentes instrucciones entrarán en vigencia a partir de la fecha de su notificación. Sin perjuicio de lo anterior, dichas instrucciones deberán ser cumplidas por las sociedades operadoras íntegramente a más tardar el 31 de diciembre 2015.

CARLOS SILVA ALLENDE
SUPERINTENDENTE DE CASINOS DE JUEGO (S)

CSA/ dal/ ltd/ rmlc
Distribución:
- Sociedades Operadoras de Casinos de Juego
- Divisiones de la SCJ
- Archivo/Oficina de Partes