IMPARTE INSTRUCCIONES RELATIVAS A LOS LINEAMIENTOS DE CIBERSEGURIDAD QUE DEBEN OBSERVAR LAS SOCIEDADES OPERADORAS Y LAS SOCIEDADES CONCESIONARIAS DE CASINOS DE JUEGO

N°	TEMA/ARTÍCULO	AUTOR OBSERVACIÓN	COMENTARIOS, OBSERVACIONES Y/O SUGERENCIAS	RESPUESTA SCJ
1	II. GESTIÓN DE LA CIBERSEGURIDAD 1 Medidas de gestión. “Toda sociedad operadora y concesionaria municipal deberá implementar medidas técnicas y de organización para gestionar los riesgos de Ciberseguridad de las redes, equipos y sistemas que utiliza para la prestación de los servicios a sus clientes, indistintamente de si tal gestión estuviere o no externalizada, los cuales deberán constar en un protocolo.”	MST	Si la gestión está externalizada, la organización que la realiza ¿debería contar con alguna certificación de algún tipo?, ¿O en su defecto los profesionales que allí laboran?	No se exige una certificación específica de la empresa externa; aun cuando es recomendable que la tenga.

2	II. GESTIÓN DE LA CIBERSEGURIDAD 1 Medidas de gestión. "Toda sociedad operadora y concesionaria municipal deberá implementar medidas técnicas y de organización para gestionar los riesgos de Ciberseguridad de las redes, equipos y sistemas que utiliza para la prestación de los servicios a sus clientes, indistintamente de si tal gestión estuviere o no externalizada, los cuales deberán constar en un protocolo."	Enjoy	Si la organización tiene la gestión externalizada ¿Debe existir alguna certificación además de los profesionales que realizan los procesos?	Ídem respuesta N°1
3	"Para todo lo anterior, se deberá considerar cualquiera de los principios y estándares internacionalmente aceptados en materia de Ciberseguridad, tales como, y sin ser taxativos, International Organization for Standarization (ISO), las recomendaciones de la OCDE incluidas en el "Digital Security Risk Management for Economic	MST	Se debería dejar más explícita esta exigencia, queda muy amplia y pareciera que fuera opcional, además indicar si se tomaran en cuenta todos estos documentos o solo algunos, y que partes de ellos.	La instrucción es obligatoria, tal como se desprende del verbo "deberá". Cabe hacer presente que no se requiere la certificación, pero sí considerar los principios o estándares asociados a materias de Ciberseguridad y seguridad de la información. Efectivamente la cláusula es amplia con el fin de ofrecer a la entidad regulada seleccionar el o los principios y estándares que mejor se adapten a su negocio.

	and Social Prosperity" (2015) y "Recommendation on Digital Security of Critical Activities" (2019)."			
4	"Para todo lo anterior, se deberá considerar cualquiera de los principios y estándares internacionalmente aceptados en materia de Ciberseguridad, tales como, y sin ser taxativos, International Organization for Standarization (ISO), las recomendaciones de la OCDE incluidas en el "Digital Security Risk Management for Economic and Social Prosperity" (2015) y "Recommendation on Digital Security of Critical Activities" (2019)."	Enjoy	Exigencia poca clara, no existen parámetros exactos por lo que se aprecia como opcional. Indicar si la solicitud de los documentos es estricta ¿todos los documentos o solo algunos? Y qué punto de los documentos se tomaran en cuenta.	Ídem respuesta N°3

5	2 Medidas de prevención y mitigación. "Las sociedades operadoras y las sociedades concesionarias de casinos de juego con el objeto de prevenir y reducir al mínimo los efectos de los ciberincidentes que afecten la seguridad de las redes, equipos, soporte tecnológico interno o externalizado y sistemas utilizados para la prestación de los servicios, con el objeto de garantizar su continuidad operativa deberán diseñar, implementar, practicar y evaluar un plan de respuesta, cuyo contenido deberá constar del protocolo antes señalado, que otorgue adecuada cobertura a sus redes, equipos y sistemas en conformidad con estándares internacionales o nacionales, de amplia aplicación, tales como los mencionados en el párrafo anterior, y, a su vez, desde el punto de vista de los clientes, se deberá promover el garantizar la integridad, disponibilidad y	MST	¿Qué información de los clientes: datos personales, datos sensibles, información de juego, ¿otros? Debería ser lo más explícito posible.	Los datos personales y datos sensibles según la ley N°19.628 de protección de datos personales. Además, de la información de juego y datos bancarios. *Respuesta implica modificación de circular

	confidencialidad de la información.”			
6	2 Medidas de prevención y mitigación. “Las sociedades operadoras y las sociedades concesionarias de casinos de juego con el objeto de prevenir y reducir al mínimo los efectos de los ciberincidentes que afecten la seguridad de las redes, equipos, soporte tecnológico interno o externalizado y sistemas utilizados para la prestación de los servicios, con el objeto de garantizar su continuidad operativa deberán diseñar, implementar, practicar y evaluar un plan de respuesta, cuyo contenido deberá constar del protocolo antes señalado, que otorgue adecuada cobertura a	Enjoy	Información con poca claridad (que tipo de información de clientes: datos personales, información de juegos).	Ídem respuesta N°5

	sus redes, equipos y sistemas en conformidad con estándares internacionales o nacionales, de amplia aplicación, tales como los mencionados en el párrafo anterior, y, a su vez, desde el punto de vista de los clientes, se deberá promover el garantizar la integridad, disponibilidad y confidencialidad de la información."			
7	3 Análisis de riesgo y seguridad por diseño. "Con el objeto de garantizar la ciberseguridad en la implementación de nuevas tecnologías, las sociedades operadoras y las sociedades concesionarias de casinos de juego, deberán considerar un conjunto de medidas de mitigación de riesgos de Ciberseguridad. Lo anterior será validado y aprobado por la alta gerencia de la sociedad operadora y concesionaria municipal, y notificado vía SAYN a la Superintendencia a los 30 días corridos siguientes	MST	¿No será necesario que las medidas sean aprobadas por el directorio en acta y posteriormente enviada a SCJ, al igual que el protocolo?.	Se incluirá la posibilidad de aprobación por el directorio o la alta gerencia, si no cuenta con directorio, especificando que se debe notificar el acta o documento en que conste la aprobación. *Respuesta implica modificación de circular

	a su implementación”.			
8	3 Análisis de riesgo y seguridad por diseño. “Con el objeto de garantizar la ciberseguridad en la implementación de nuevas tecnologías, las sociedades operadoras y las sociedades concesionarias de casinos de juego, deberán considerar un conjunto de medidas de mitigación de riesgos de Ciberseguridad. Lo anterior será validado y aprobado por la alta gerencia de la sociedad operadora y concesionaria municipal, y notificado vía SAYN a la Superintendencia a los 30 días corridos siguientes a su implementación”.	Enjoy	Sería ideal saber el detalle de las medidas de mitigación de riesgos de ciberseguridad a la que hacen referencia	No se exigen medidas de mitigación específicas, ya que estas dependen directamente de los riesgos intrínsecos de cada institución, los cuales pueden ser distintos entre cada una de ellas. Es por ello que se deja a criterio de cada institución el determinar estas medidas en base a su análisis de riesgo. Sin perjuicio de lo anterior, recomendamos tener a la vista al menos los framework ISO 27.002 o NIST. Sin embargo, las siguientes son el conjunto de materias mínimas a considerar en los análisis: <u>Controles organizacionales</u> • Políticas de seguridad de la información • Roles y responsabilidades de seguridad de la información • Segregación de deberes • Responsabilidades de gestión • Contacto con autoridades • Contacto con grupos de interés especial • Inteligencia de amenazas • Seguridad de la información en la gestión de proyectos

				• Inventario de información y otros activos asociados • Uso aceptable de información y otros activos asociados. • Retorno de activos • Clasificación de la información • Etiquetado de información • Transferencia de información • Control de acceso • Gestión de identidad • Información de autenticación • Derechos de acceso • Seguridad de la información en las relaciones con los proveedores • Abordar la seguridad de la información dentro de los acuerdos con proveedores • Gestión de la seguridad de la información en la cadena de suministro de las TIC • Seguimiento, revisión y gestión de cambios de los servicios de proveedores. • Seguridad de la información para el uso de servicios en la nube • Planificación y preparación de la gestión de incidentes de seguridad de la información • Evaluación y decisión sobre eventos de seguridad de la información • Respuesta a incidentes de seguridad de la información • Aprendiendo de los incidentes de seguridad de

				la información • Recolección de evidencia • Seguridad de la información durante la interrupción • Preparación de las TIC para la continuidad empresarial • Identificación de requisitos legales, estatutarios, regulatorios y contractuales • Derechos de propiedad intelectual • Protección de registros • Privacidad y protección de datos personales o sensibles • Revisión independiente de la seguridad de la información • Cumplimiento de políticas y estándares de seguridad de la información • Procedimientos operativos documentados Controles de personas • Verificación de personal respecto de sus capacidades y habilidades para los roles asignados • Términos y condiciones de empleo • Sensibilización, educación y formación en seguridad de la información • Proceso Disciplinario • Responsabilidades después de la terminación o cambio de empleo • Acuerdos de confidencialidad o no divulgación • Trabajo remoto • Informes de eventos de seguridad de la

				información <u>Controles físicos</u> • Perímetro de seguridad física • Controles de entrada física • Asegurar oficinas, salas e instalaciones • Monitoreo de seguridad física • Protección contra amenazas físicas y ambientales • Trabajando en áreas seguras • Escritorio despejado y pantalla despejada • Ubicación y protección de equipos • Seguridad de los activos fuera de las instalaciones • Medios de almacenamiento • Utilidades de apoyo • Seguridad del cableado • Mantenimiento de equipo • Eliminación o reutilización segura de equipos <u>Controles tecnológicos</u> • Dispositivos endpoint de usuario • Derechos de acceso privilegiado • Restricción de acceso a la información • Acceso al código fuente • Autenticación segura • Gestión de capacidad • Protección contra malware • Gestión de vulnerabilidades técnicas • Gestión de la configuración • Eliminación de información

				• Enmascaramiento de datos • Prevención de fuga de datos • Respaldo de información • Redundancia de instalaciones de procesamiento de información • Inicio sesión • Actividades de seguimiento • Sincronización de reloj • Uso de programas de utilidad privilegiados • Instalación de software en sistemas operativos • Controles de red • Seguridad de los servicios de red • Filtrado web • Segregación en redes • Uso de criptografía • Ciclo de vida de desarrollo seguro • Requisitos de seguridad de la aplicación • Principios de ingeniería y arquitectura de sistemas seguros • Codificación segura • Pruebas de seguridad en desarrollo y aceptación • Desarrollo subcontratado • Separación de entornos de desarrollo, prueba y producción • Gestión del cambio • Información de prueba • Protección de los sistemas de información durante la auditoría y las pruebas.

				*Requiere modificación de circular aclarando la materia en un anexo.
9	"Para la implementación de nuevas tecnologías, las sociedades operadoras y las sociedades concesionarias de casinos de juego, deberán adoptar las medidas tendientes a garantizar la operación y seguridad de las partes sensibles de sus sistemas, redes y equipos, así como también la obligación de resguardar la confidencialidad, disponibilidad e integridad de la información que se transmita y almacene por sus tecnologías, las que podrán ser acreditadas por cualquier medio para efectos de fiscalización por parte de la SCJ."	MST	Dice "…por cualquier medio", favor de explicitar cuales serían estos.	Los medios por los que se puede probar es declaración de testigos, documentos, grabaciones, entre otros.

10	"Para la implementación de nuevas tecnologías, las sociedades operadoras y las sociedades concesionarias de casinos de juego, deberán adoptar las medidas tendientes a garantizar la operación y seguridad de las partes sensibles de sus sistemas, redes y equipos, así como también la obligación de resguardar la confidencialidad, disponibilidad e integridad de la información que se transmita y almacene por sus tecnologías, las que podrán ser acreditadas por cualquier medio para efectos de fiscalización por parte de la SCJ."	Enjoy	Agradecemos detallar a que medios de fiscalización se refieren.	Se fiscalizará la aplicación y consideración de dichas medidas y dicha obligación por parte de la unidad de ciberseguridad y los empleados del casino, lo que puede ser acreditado por declaración de testigos, documentos, grabaciones, entre otros.
11	4 Planes de gestión de riesgo. "Se entregará a la Superintendencia una copia del acta donde conste la realización de la presentación, de la cual se podrá omitir la información no pertinente a ciberseguridad, y que será tratada con la debida reserva."	MST	¿Corresponde a un Acta de directorio o solo un acta como respaldo de la actividad?	Si la sociedad cuenta con directorio corresponde un acta de su sesión. Si la sociedad solo opera con alta gerencia, basta un acta de reunión. *Requiere modificación de circular aclarando naturaleza del acta.

12	4 Planes de gestión de riesgo. "Se entregará a la Superintendencia una copia del acta donde conste la realización de la presentación, de la cual se podrá omitir la información no pertinente a ciberseguridad, y que será tratada con la debida reserva."	Enjoy	No entendemos este punto. Agradecemos detallar.	Se refiere al acta de la sesión del directorio o de la reunión de la alta gerencia, en que los planes de gestión de riesgo que son revisados o actualizados son sometidos a su conocimiento y aprobación. *Requiere modificación de circular aclarando la materia
13	III UNIDADES DE CIBERSEGURIDAD 1°. Unidades de ciberseguridad "Las sociedades operadoras y las sociedades concesionarias de casinos de juego deberán contar con una Unidad de Ciberseguridad, cuyo responsable será la contraparte técnica ante esta SCJ y deberá contar con las competencias suficientes para velar por la observancia de las obligaciones previstas en la presente circular, identificar los riesgos de afectación de los servicios por causa de ciberincidentes, verificar el cumplimiento eficaz de los	MST	¿Cuáles serían las "competencias suficientes" del responsable?	Competencias mínimas para el rol: • Desarrollar y comunicar políticas, estándares y pautas de seguridad de la información corporativa. Contribuir al desarrollo de estrategias organizacionales que abordan los requisitos de control de la información. Identificar y monitorear las tendencias ambientales y del mercado y evaluar proactivamente el impacto en las estrategias, beneficios y riesgos comerciales. Liderar la provisión de asesoramiento y orientación autorizados sobre los requisitos para los controles de seguridad en colaboración con expertos en otras funciones, como soporte legal y técnico. Asegurar que los principios arquitectónicos se apliquen durante el diseño para reducir el riesgo e impulsar la adopción y el cumplimiento de políticas, estándares y pautas. • Proporcionar asesoramiento y orientación sobre estrategias de seguridad para gestionar los riesgos identificados y garantizar la adopción y el

	respectivos planes de gestión, reportar los ciberincidentes y coordinar la gestión de ciberseguridad en general. Los roles y responsabilidades contempladas en esta Unidad deberán constar por escrito en el mismo Protocolo señalado en el numeral II.”			cumplimiento de los estándares. Obtener y actuar sobre la información de vulnerabilidad y realizar evaluaciones de riesgos de seguridad, análisis de impacto empresarial y acreditación en sistemas de información complejos. Investigar las principales brechas de seguridad y recomendar las mejoras de control adecuadas. • Explicar el propósito y brindar asesoramiento y orientación sobre la aplicación y operación de controles elementales de seguridad físicos, procedimentales y técnicos. Realizar evaluaciones de riesgos de seguridad, vulnerabilidades y análisis de impacto empresarial para sistemas de información de complejidad media. Investigar presuntos ataques y gestionar incidentes de seguridad. Utilizar análisis forense cuando sea apropiado. • Comunicar los riesgos y problemas de seguridad de la información a los gerentes comerciales y otros. Aplicar y mantener controles de seguridad específicos según lo requiera la política de la organización y las evaluaciones de riesgos locales. Investigar presuntos ataques. Responder a las brechas de seguridad de acuerdo con la política de seguridad y registrar los incidentes y las acciones tomadas. • Competencias sobre gobierno de la seguridad de la información • Competencias sobre gestión de riesgos de seguridad de la información

				• Competencias sobre el desarrollo y gestión de un programa de seguridad de la información • Competencias sobre gestión de incidentes de seguridad de la información • Conocimientos sobre marcos legales atingentes a seguridad de la información y ciberseguridad • Conocimiento sobre marcos normativos nacionales e internacionales sobre ciberseguridad Estos aspectos se verificarán con alguna o todas estas posibilidades. - Deseable certificación CISM o equivalente - Deseable certificación CISSP o equivalente - Deseable certificación Implementador ISO27001 o equivalente - Deseable Diplomados en Gestión de Seguridad de la Información - Deseable Magister o Doctorado en Seguridad de la información - Necesaria experiencia laboral verificable en seguridad de la información - Carrera deseables: Ingeniería en Informática, Ingeniería Electricista, Abogado con experiencia en ciberseguridad y datos o Electrónica, Ingenierías en Ciberseguridad o afín. *Respuesta implica modificación de circular como anexo

14	III UNIDADES DE CIBERSEGURIDAD 1°. Unidades de ciberseguridad "Las sociedades operadoras y las sociedades concesionarias de casinos de juego deberán contar con una Unidad de Ciberseguridad, cuyo responsable será la contraparte técnica ante esta SCJ y deberá contar con las competencias suficientes para velar por la observancia de las obligaciones previstas en la presente circular, identificar los riesgos de afectación de los servicios por causa de ciberincidentes, verificar el cumplimiento eficaz de los respectivos planes de gestión, reportar los ciberincidentes y	Enjoy	¿Cómo se medirán las competencias suficientes del responsable? favor detallar.	Ídem respuesta 13.

	coordinar la gestión de ciberseguridad en general. Los roles y responsabilidades contempladas en esta Unidad deberán constar por escrito en el mismo Protocolo señalado en el numeral II.”			
15	“Las sociedades operadoras y las sociedades concesionarias de casinos de juego deberán notificar a esta Superintendencia las identidades y medios de contacto del o la titular y suplente de la Unidad de Ciberseguridad, dentro de los 10 días siguientes a la entrada en vigencia de esta circular. En el mismo plazo se deberá proceder ante modificaciones en dichos cargos.”	MST	Cuando se refiere a la notificación del personal titular y suplente, ¿considera 10 días hábiles o corridos?, por otra parte, ¿la designación deberá quedar respaldada en acta de directorio?	Se considera días hábiles administrativos. No es necesario que la designación esté en el acta de directorio, pero si no consta en ésta, deben ser consideradas estas funciones en el contrato individual de las personas que ostenten dichos cargos. *Requiere modificación de circular aclarando la materia.

16	"Las sociedades operadoras y las sociedades concesionarias de casinos de juego deberán notificar a esta Superintendencia las identidades y medios de contacto del o la titular y suplente de la Unidad de Ciberseguridad, dentro de los 10 días siguientes a la entrada en vigencia de esta circular. En el mismo plazo se deberá proceder ante modificaciones en dichos cargos."	Enjoy	Cuando se refiere a la notificación del personal titular y suplente, ¿considera 10 días hábiles o corridos?, por otra parte, ¿Cuál sería la forma de notificación?	Se considera días hábiles administrativos. No es necesario que la designación esté en el acta de directorio, pero si no consta en ésta, deben ser consideradas estas funciones en el contrato individual de las personas que ostenten dichos cargos. Por otro lado, se habilitará un formulario en SAYN para estas notificaciones. *Requiere modificación de circular aclarando la materia.
17	IV REPORTE OBLIGATORIO DE CIBERINCIDENTES 1°. Obligación de reportar ciberincidentes "…Las sociedades operadoras y las sociedades concesionarias de casinos de juego deberán reportar a la Superintendencia y los ciberincidentes que detecte en sus redes, equipos y sistemas y que alcancen los Niveles de peligrosidad e impacto establecidos en esta circular sin perjuicio de las	MST	¿Todo reporte solicitado en el presente documento, será en plataforma SAYN?	Sí, se habilitará un formulario en SAYN para estas notificaciones.

	instrucciones precisas que emita la Superintendencia respecto de tipos específicos de incidentes".			
18	c. Ciberincidentes de reporte obligatorio "Además, las sociedades operadoras y las sociedades concesionarias de casinos de juego deberán notificar a la Superintendencia los incidentes de ciberseguridad que afecten a proveedores de máquinas de azar, tan pronto tengan conocimiento de ellos."	MST	El tipo de reporte de estos ciberincidentes, ¿deberá basarse en los criterios descritos en las tablas 1 y 2? Sería bueno que se detallase un formato para esto o el nivel de detalle requerido.	Efectivamente, la notificación se base en tablas 1 y 2. El formulario SAYN contemplará los campos requeridos. *Requiere modificación de circular aclarando la materia.
19	IV. REPORTE OBLIGATORIO DE CIBERINCIDENTES 1°. Obligación de reportar ciberincidentes	Enjoy	¿Cuál sería la forma de notificación?	El formulario SAYN será el medio para notificar los ciberincidentes.

20	V Información a terceros e intercambio de información 1°. Información a terceros e intercambio de información En caso de reportar y/o alertar a terceros para prevenir, gestionar o resolver un ciberincidente, la sociedad operadora o concesionaria municipal podrá solicitar, por intermedio de la Superintendencia, la asistencia del CSIRT, el que actuará conforme a su disponibilidad. En caso de requerir apoyo de Equipos de Respuesta en el extranjero, se deberá velar por la privacidad y el debido resguardo de los datos personales involucrados.	MST	El reporte podría ser en paralelo, tanto a la Superintendencia, como al CSIRT, dada la criticidad del incidente, por ejemplo, en caso de que sea fuera del horario de operación normal de la SCJ. ¿La superintendencia informará a las sociedades operadoras, el protocolo que tendrá con el CSIRT?	Las comunicaciones entre las sociedades operadoras y el CSIRT de Gobierno se efectuarán por intermedio de la Superintendencia de Casinos de Juego y el Sistema de Autorizaciones y Notificaciones de la Superintendencia (SAYN). En el respectivo formulario que se cree al efecto, se deberá indicar el grado de confidencialidad de la información compartida según el protocolo TLP, el cual se adjunta en anexos de la circular para entendimiento y estará disponible al momento de reportar los ciberincidentes. Por otro lado, y respecto de aquellos ciberincidentes que atendida su gravedad requieran de acciones inmediatas según su nivel de impacto y peligrosidad y que se produzcan en horas en que la SCJ se encuentre fuera de su horario operativo, podrán ser notificadas conjuntamente al CSIRT y a la SCJ haciendo uso de la plataforma SAYN a través de formulario y opción que será habilitada al efecto.
21	VI Resolución de ciberincidentes 1. Obligación de resolución de ciberincidentes	Forensic & Cybercrime	Teniendo en consideración que actualmente los casinos de juego en su actividad comercial se encuentran sujetos a riesgos de ciberseguridad, donde podrían ser víctimas de ciberataques o ciberdelitos, es que se hace imprescindible que los casinos de juego cuenten con todos los medios para realizar una investigación forense adecuadamente y un correcto tratamiento de la evidencia digital, para tener la certeza que puedan presentar evidencia con alto valor probatorio en procesos judiciales y así perseguir eficientemente responsabilidades de los cibercriminales tanto internos como	Se incluirá un párrafo similar, redactado en forma facultativa. El verbo rector será “podrá”, ya que es deseable, pero no obligatorio. *Requiere modificación de circular aclarando la materia.

			externos. Se propone que las etapas mencionadas se alinean con las utilizadas internacionalmente, en normas técnica tales como: • ISO/IEC 27043:2015 Information technology — Security techniques — Incident investigation principles and processes • ISO/IEC 27042:2015 Information technology — Security techniques — Guidelines for the analysis and interpretation of digital evidence • ISO/IEC 27037:2012 Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence Como tampoco con las normas técnicas nacionales publicadas por el Instituto Nacional de Normalización, tales como: • NCh-ISO27037:2015 Tecnología de la información - Técnicas de seguridad - Directrices para la identificación, recopilación, adquisición y preservación de evidencia digital • NCh-ISO IEC 27042:2019 Tecnología de la información - Técnicas de seguridad – Directrices para el análisis e interpretación de evidencia digital • NCh-ISO IEC 27043:2018 Tecnología de la información - Técnicas de seguridad - Principios y procesos de investigación de incidents Párrafo propuesto por Forensic & Cybercrime“Las sociedades operadoras y las sociedades concesionarias de casinos de juego deberán realizar un proceso de investigación forense para los ciberincidentes relevantes, ciberataques y ciberdelitos, efectuados tanto por personal interno como también desde el exterior. Que	

			considere al menos las etapas de identificación, recopilación, adquisición, examen y análisis de evidencias digitales, junto con la generación de documentación e informes de la investigación forense, interpretación de evidencia digital y las conclusiones del trabajo realizado; además de cumplir los requerimientos necesarios para preservar y realizar adecuadamente la cadena de custodia de las evidencias digitales obtenidas y generadas. Este proceso de investigación forense debe ser realizado exclusivamente por personal con competencias comprobables, como también con absoluta independencia e imparcialidad, para asegurarse que sus análisis, interpretaciones y conclusiones sean libres de sesgos, como también de eventuales presiones indebidas".	
22	VI Resolución de ciberincidentes 1. Obligación de resolución de ciberincidentes	Forensic & Cybercrime	Teniendo en consideración la importancia de los registros históricos (logs) para proceso de investigación forense exitoso frente a ciberincidentes relevantes, ciberataques y ciberdelitos efectuados tanto por personal interno como también desde el exterior, es que el requerimiento de la existencia y calidad de registros históricos (logs) debería ser explicita. Esto debería aplicar tanto para sistemas e infraestructura interna, servicios externalizados y servicios/tecnologías contratadas. Párrafo propuesto por Forensic & Cybercrime "Las sociedades operadoras y las sociedades concesionarias de casinos de juego deberán diseñar, implantar y mantener controles de protección y detección para facilitar el proceso de investigación forense, entre los que se encuentra gestionar el ciclo de vida completo de registros históricos (logs) en aspectos tales como: existencia, nivel de detalle, consistencia de su información, período de resguardo y modo de resguardo, como también realizar	Se acepta parcialmente. Se incluirá la obligación de resguardo por seis meses. Cumplido tres años de vigencia de la circular, se ampliará el plazo a un año. *Requiere modificación de circular aclarando la materia.

			periódicamente pruebas de trazabilidad para asegurar su calidad y que serán de utilidad al momento de ser requeridos para una investigación forense. Esto es aplicable para tanto para sistemas e infraestructura interna, servicios externalizados, y servicios o tecnologías contratadas".	
23	VIII Supervisión de seguridad 1. Supervisión de seguridad "Las sociedades operadoras y las sociedades concesionarias de casinos de juego deberán someter regularmente sus redes, equipos y sistemas a pruebas de seguridad, con la frecuencia que corresponda de acuerdo con el plan de riesgo aprobado y sancionado por su alta dirección, conforme al numeral II.4. de esta circular…"	MST	Se podría definir una periodicidad base, al menos como ejemplo para la aplicación de esta medida.	Se definirá que se realice a lo menos semestralmente, debiendo ser informada a la SCJ a más tardar 15 días hábiles de realizadas. *Requiere modificación de circular aclarando la materia.

24	IX. DISPOSICIONES FINALES 3 Entrada en vigencia “La presente circular entrará en vigencia transcurrido tres meses contados desde su dictación”.	MST	Debería ser al menos 6 meses, considerando la selección del personal idóneo, la inducción respecto de los sistemas de la Sociedad Operadora, además del levantamiento y creación de protocolos, aprobación del directorio, respaldos, entre otros. Se debería considerar una primera visita de fiscalización como marcha blanca, objeto de ayudar y orientar a las sociedades operadoras, en la correcta implementación de la presente circular.	De acuerdo, nos parece razonable *Requiere modificación de circular aclarando la materia.
25	IX. DISPOSICIONES FINALES 3. Entrada en vigencia	Enjoy	Se sugiere entrada en vigencia transcurridos seis meses contados desde su dictación.	Ídem respuesta N°24