Normativa en Consulta de la Superintendencia de Casinos de Juego, circular Ciberseguridad.

En contexto de normativa en consulta "Circular de Ciberseguridad, a continuación, se detallan comentarios sobre la normativa:

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.*"

Comentario:

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?.

"*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).*"

Comentario:

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.

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 confidencialidad de la información.*"

Comentario:

¿Qué información de los clientes: datos personales, datos sensibles, información de juego, ¿otros? Debería ser lo más explícito posible.

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".

Comentario:

¿No será necesario que las medidas sean aprobadas por el directorio en acta y posteriormente enviada a SCJ, al igual que el protocolo?.

"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."

Comentario:

Dice "…por cualquier medio", favor de explicitar cuales serían estos.

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."

Comentario:

¿Corresponde a un Acta de directorio o solo un acta como respaldo de la actividad?

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 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."

Comentario:

¿Cuáles serían las "competencias suficientes" del responsable?

"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."

Comentario:

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?

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 instrucciones precisas que emita la Superintendencia respecto de tipos específicos de incidentes".

Comentario:

¿Todo reporte solicitado en el presente documento, será en plataforma SAYN?

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.*"

Comentario:

El tipo de reporte de estos ciberincidentes, ¿deberá basarse en los criterios descritos en las tablas 1 y 2? Seria bueno que se detallase un formato para esto o el nivel de detalle requerido.

3. Oportunidad de los Reportes

Comentario:

En la periodicidad de los reportes, no queda claro si se debe elegir la periodicidad entre los valores dados en la tabla, o se debe seguir el orden indicado en la tabla.

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.

Comentario:

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?

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…"

Comentario:

Se podría definir una periodicidad base, al menos como ejemplo para la aplicación de esta medida.

IX. DISPOSICIONES FINALES
3 Entrada en vigencia

"La presente circular entrará en vigencia transcurrido tres meses contados desde su dictación".

Comentario:

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.