Comentario 1

Cláusula normativa

VI Resolución de ciberincidentes

1. Obligación de resolución de ciberincidentes

Comentarios específicos

1.1 Teniendo en consideración que actualmente los casinos de juego en su actividad comercial se encuentran sujetos a riesgos de ciberseguridad, donde podrían ser victimas 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 externos.

1.2 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 incidentes

Párrafo propuesto

“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”.

Comentario 2

Cláusula normativa

VI Resolución de ciberincidentes

1. Obligación de resolución de ciberincidentes

Comentarios específicos

2.1 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

“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 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”.