SCJ | SUPERINTENDENCIA DE CASINOS DE JUEGO

CIRCULAR INTERNA N° 7

MAT.: Instruye procedimiento de reporte de incidentes de seguridad de la información.

ANT.: 1) Res. Exenta N°450 de 20.07.2012 que establece Comité de Gestión de Riesgos y de Seguridad de la Información, define roles y aprueba las políticas de gestión de riesgos y de seguridad de la información, y Res. Exenta N°234 de 29.05.2013 que modifica Resolución que establece el Comité de Gestión de Riesgos y de Seguridad de la Información, y modifica Política de Seguridad de la Información.

2) D.S. N°83 publicado el 12.01.2005 y D.S. N°93 publicado el 28.07.2006, ambos del Ministerio Secretaría General de la Presidencia.

SANTIAGO, 17 SEP 2013

VISTOS; lo dispuesto en el artículo 31 del D.F.L. N° 1/19.653 que fija el texto refundido, coordinado y sistematizado de la Ley N° 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado; el numeral 1 del artículo 42 de la Ley Nº 19.995 sobre Bases Generales para la Autorización, Funcionamiento y Fiscalización de Casinos de Juego; el Decreto Supremo N° 83, de 2005, del Ministerio Secretaría General de la Presidencia, que Aprueba Norma Técnica para los Órganos de la Administración del Estado sobre Seguridad y Confidencialidad de los Documentos Electrónicos; el Oficio GAB. PRES. N° 007 de S.E. la Presidenta de la República, de 4 de diciembre de 2006; el Decreto Supremo N° 573, así como en las demás disposiciones pertinentes; dicto lo siguiente:

CONSIDERANDO:

1.- Que le corresponde a este Superintendente dirigir y organizar el funcionamiento de la Superintendencia.

2.- Que la misión institucional de este Organismo de Control consiste en regular a la industria de casinos de juego, promoviendo su desarrollo eficiente, responsable y transparente; efectuando una supervigilancia de calidad que garantice el íntegro cumplimiento de la normativa y resguarde, entre otros bienes jurídicos, la fe pública, el orden público, el pago de impuestos y la contribución al desarrollo regional, mediante funcionarios y procesos de excelencia.

SCJ | SUPERINTENDENCIA DE CASINOS DE JUEGO

3.- Que en esas circunstancias, atendido el actual nivel de desarrollo de la industria de casinos de juego y los crecientes grados de complejidad que ha alcanzado el ejercicio de la labor fiscalizadora, a juicio de esta autoridad, resulta indispensable fortalecer el compromiso de esta Superintendencia en orden a desarrollar y mantener una eficiente Política de Seguridad de la Información, a fin de reducir los riesgos los riesgos de seguridad de la información.

4. Que con fecha 30 de julio de 2012 esta autoridad dictó la Resolución Exenta N° 0450 que, entre otras materias, crea el "Comité de Gestión de Riesgos y de Seguridad de la Información", define su metodología, funcionamiento y responsabilidades; aprueba la Política de Gestión de Riesgos de la Superintendencia de Casinos de Juego; y aprueba la Política General de Seguridad de la Información de esta Superintendencia, la que fue modificada por medio de la Resolución Exenta N°234 de 29.05.2013, en la cual se informa en su numeral "XI NORMAS QUE COMPONEN LA POLÍTICA", que se debe desarrollar una Norma de Gestión de Incidentes de Seguridad de la Información, la que se compone de procedimientos.

5.- Que, por otro lado, el Superintendente de Casinos de Juego, siguiendo las directrices en materia de seguridad de la información contenidas en el artículo 20 del Decreto Supremo N° 83, de 2005 del Ministerio Secretaría General de la Presidencia, debe impartir instrucciones para la seguridad de los documentos electrónicos, incluyendo entre éstas, procedimientos para reportar incidentes de seguridad, para lo cual, entre otras acciones, se ha incorporado el sistema de seguridad de la información a las metas de eficiencia institucional de esta Superintendencia a partir del año 2012.

6.- Que, en mérito de lo expuesto en los considerandos precedentes,

RESUELVO:

1.- IMPÁRTASE el siguiente:

PROCEDIMIENTO PARA EL REPORTE DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

1. OBJETIVO

La presente Circular Interna, tiene por objeto establecer mecanismos y acciones claras y efectivas, mediante las cuales, los funcionarios de la Superintendencia reporten cualquier tipo de incidente de Seguridad de la Información que ocurran tanto al interior de la Superintendencia, como en los equipos propiedad de la institución y que no necesariamente estén al interior de ésta. Lo anterior con el fin de disminuir al máximo posible el tiempo de respuesta y las consecuencias producidas por este tipo de eventos y con esto asegurar el eficiente cumplimiento de los objetivos de la institución.

2. ALCANCE

La presente Circular se aplica a todos los incidentes que comprometan la integridad, confidencialidad o disponibilidad de los activos de información y sistemas institucionales que apoyan la ejecución de la misión Institucional.

Para estos efectos se definen como activos de información, los cuales son objeto de reporte de incidentes de seguridad de la información, a todos aquellos elementos que participan en la creación, manipulación, procesamiento y almacenamiento de la información, de decir equipos, programas y documentos. Estos últimos en sus diversos formatos: papel, digital, magnético, gráfico y en sus diversos reservorios: bases de datos, archivos, bodegas, etc.

Las acciones aquí señaladas aplican a todos los funcionarios, proveedores, contratistas y, personal vinculado con los proveedores que presten servicios a la Superintendencia de Casinos de Juego y sus subcontratados.

3. RESPONSABILIDADES

La ejecución de las actividades aquí detalladas es responsabilidad de los funcionarios, proveedores, contratistas y personal vinculado con los proveedores que presten servicios a la Superintendencia de Casinos de Juego y sus subcontratados, a quienes deberá hacerse conocida la presente mediante correo electrónico del Oficial de Seguridad de la Información dirigido a la contraparte del respectivo contrato.

La verificación del cumplimiento del presente procedimiento será responsabilidad del Oficial de Seguridad o quien cumpla la señalada función. Además será responsable de gestionar los recursos necesarios para que, las personas señaladas en el párrafo anterior, implementen de forma efectiva las estrategias y procedimientos de respuesta a incidentes de seguridad de la información.

4. DESARROLLO

Un incidente de seguridad de la información se define como cualquier evento o situación que compromete de manera importante la confidencialidad, integridad o disponibilidad, de un activo de información institucional de carácter crítico, y que puede ser causado por exposición de alguna vulnerabilidad o amenaza de violar los mecanismos de seguridad existentes; o una violación a la Política de Seguridad de la Información Institucional.

El reporte de los incidentes permite responder a los mismos en forma sistemática, minimizar su ocurrencia, facilitar una recuperación rápida y eficiente de las actividades minimizando la pérdida de información y la interrupción de los servicios, mejorar continuamente el marco de seguridad y el procedimiento para tratamiento de incidentes, y manejar correctamente los aspectos legales que pudieran surgir durante este proceso.

Los incidentes de seguridad de la información que deben ser siempre reportados son:

- Código malicioso;

- Acceso no autorizado

- Acceso no autorizado o problemas con el correo electrónico

- Robos de información

- Mal uso de los recursos informáticos

- Uso de software no autorizado.

- Pérdida de información en caso de (i) Incendio; (ii) Inundación; (iii) Terremoto; (iv) Asalto o robo.

Además de los incidentes de seguridad de la información antes señalados, se podrán definir nuevos incidentes que la institución estime conveniente.

Todos los incidentes que puedan afectar la seguridad de la información, deben ser informados inmediatamente al Jefe de la Unidad Informática y Oficial de Seguridad de la Información, mediante correo electrónico. En caso de no encontrarse disponible, se deberá informar mediante la misma vía a cualquier integrante de la Unidad Informática, debiendo además procurar que el Jefe de la Unidad de Informática y el Oficial de Seguridad de la Información, también estén copiados en el señalado reporte.

El reporte señalado deberá considerar lo siguiente:

- Identificación del usuario que presenta el incidente.
- Fecha del incidente.
- Hora del incidente.
- Indicios del incidente.

Una vez solucionado el incidente, se registrará en el informe de cierre la solución que se dio al mismo y las medidas preventivas tomadas para que dicho incidente no se vuelva a repetir.

Finalmente, el Jefe de la Unidad Informática y el Oficial de Seguridad de la Información, deben mantener un registro actualizado, de todos los incidentes de seguridad reportados, con su adecuado seguimiento y mejora o reacción que se haya tomado para su solución, y la descripción de las medidas preventivas para que éste no se repita.

5.- DIFUSIÓN

El presente procedimiento deberá hacerse conocido a quienes corresponda, mediante las siguientes vías:

- La presente circular interna.
- Publicación en la Intranet de la Superintendencia.
- Correo electrónico del Oficial de Seguridad de la Información.

SCJ | SUPERINTENDENCIA DE CASINOS DE JUEGO

6.- RECOMENDACIONES

Como primera medida, siempre que se sospeche de una intrusión en un computador institucional, éste debe ser desconectado inmediatamente de la red (desconectando el cable correspondiente o desconectándose de la red Wifi).

7.- VIGENCIA

La presente Circular entrará en vigencia a contar de su dictación.-

Anótese, comuníquese y archívese.

SUPERINTENDENCIA DE CASINOS DE JUEGO

RENATO HAMEL MATURANA
SUPERINTENDENTE DE CASINOS DE JUEGO

MLC/CSA/PFI