SCJ | SUPERINTENDENCIA DE CASINOS DE JUEGO

E12739/2016

SUPERINTENDENCIA DE CASINOS DE JUEGO
28 DIC 2016
TOTALMENTE TRAMITADO DOCUMENTO OFICIAL

REF.: APRUEBA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN RESPECTO RELACIONES CON TERCEROS DE LA SUPERINTENDENCIA DE CASINOS DE JUEGO.

RESOLUCIÓN EXENTA Nº 556

SANTIAGO, 28 DIC 2016

VISTOS:

Lo dispuesto en la ley Nº 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado; la Ley Nº 18.834, sobre Estatuto Administrativo; en la Ley N° 20.212 de 2007 que modifica las leyes 19.553, 19.882 y otros cuerpos legales con el objeto de incentivar el desempeño de funcionarios públicos; en la Ley Nº 19.995 que establece las bases generales para la autorización, funcionamiento y fiscalización de casinos de juego; en lo dispuesto en la Ley Nº 19.799, sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma; en el Decreto 181/2002, que aprueba el Reglamento de la Ley N° 19.799 sobre documentos electrónicos, firma electrónica y la certificación de dicha firma; en el Decreto Nº 83/2004 del Ministerio Secretaria General de la Presidencia que aprueba norma técnica para los órganos de la administración del estado sobre seguridad y confidencialidad de los documentos electrónicos; en la Resolución Nº 1 .600, de la Contraloría General de la República que fija normas sobre exención del trámite de toma de razón; y en la Resolución Exenta Nº 450 de 30 de julio de 2012, de esta Superintendencia 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.

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.

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 políticas eficientes que garanticen el resguardo y uso de los activos de información institucional.

4.- Que, el artículo 11 bis de la Ley Nº 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado dispone que los funcionarios de la Administración del Estado deberán observar el principio de probidad administrativa y, en particular, las normas legales generales y especiales que lo regulan.

5.- Que, del mismo modo, el DFL. Nº 29, de 2005, del Ministerio de Hacienda, que fija texto refundido, coordinada y sistematizado de la ley Nº 18.834, sobre Estatuto Administrativo, en la letra g de su artículo 61, dispone que será obligación de cada funcionario observar estrictamente el principio de probidad administrativa, que implica una conducta funcionaria moralmente intachable y una entrega honesta y leal al desempeño de su cargo, con preeminencia del interés público sobre el privado.

6.- Que por otro lado, la Superintendencia de Casinos de Juego, siguiendo las directrices en materia de seguridad de la información contenida en el Decreto Supremo Nº 83, de 2004 del Ministerio Secretaría General de la Presidencia, debe establecer y mantener actualizados estándares mínimos de seguridad en el uso, almacenamiento, acceso y distribución de documentos electrónicos.

7.- Que en mérito de lo expuesto en los considerandos precedentes y en uso de las facultades que me confiere la ley,

RESUELVO:

ARTICULO 1°. - Establézcase la Política de Seguridad de la Información respecto relaciones con terceros, que continuación se señala:

A. DEL OBJETIVO DE LA POLÍTICA

El propósito de esta política es definir las normas generales que, desde la perspectiva de la seguridad de información, deben considerarse en:

- La relación de los funcionarios con terceros;
- La contratación y administración de servicios externos.

Así, los servicios entregados por terceros deben ser considerados como activos de información y como tales, deben ser sometidos a evaluaciones de riesgo periódicas, tomándose e implementándose medidas de acuerdo a los resultados de la revisión.

B. DEL ALCANCE DE LA POLÍTICA

Todos los funcionarios de la Superintendencia de Casinos de Juego, empresas contratistas, regulados y ciudadanos, deberán guiar su actuar por la presente política, la que se aplicará particularmente sobre los activos cuyo análisis de criticidad tenga como resultado "Alto", en el inventario de activos institucional.

C. DEL MARCO REFERENCIAL DE LA POLÍTICA

La presente política dice relación con:

- Política General de Seguridad de la Información.
- Circular Interna N°3/2016 que "Establece Protocolo que contiene las instrucciones y órdenes relativas a las formas de comunicación entre los funcionarios de la Superintendencia de Casinos de Juegos y los interesados en el proceso de otorgamiento de permisos de operación de un Casino de Juegos (2016)".

D. DE LA REVISION DE LA POLÍTICA

La presente política, deberá ser revisada y/o actualizada ante la ocurrencia de cualquiera de los siguientes hitos:

- Inicio de un proceso de otorgamiento de Permisos de Operación
- Término de un proceso de Otorgamiento de Permisos de Operación.
- Cada vez que se produzcan cambios en la Política General de Seguridad de la Información institucional.
- Ocurrencia de una violación a la política.

Asimismo, la presente política deberá ser revisada y/o actualizada cada vez que se produzcan cambios en la Política General de Seguridad de la Información institucional. En caso que ésta última política no sufra modificaciones durante dos años, al finalizar dicho período, el encargado de seguridad revisará la presente

política y sugerirá al Comité de Gestión de Riesgo y Seguridad de la Información los cambios que fuesen pertinentes.
Además, anualmente el encargado de seguridad institucional revisará el cumplimiento efectivo y la aplicabilidad de la presente política; y sugerirá al Comité de Gestión de Riesgo y Seguridad de la Información los cambios que fuesen pertinentes.
Todas las correcciones aprobadas deberán ser registradas por el encargado de seguridad en un informe que contenga la información presentada en la letra H del presente documento.

E. DE LA DIFUSIÓN DE LA POLÍTICA

Desde su entrada en vigencia y cada vez que la presente política sea actualizada deberá ser distribuida a todos los funcionarios vía correo electrónico, y publicada en la Intranet, manteniéndose en dicho estado durante toda su vigencia. Además deberá estar disponible para todos los proveedores y terceros interesados.

F. DE LOS ROLES Y SUS RESPONSABILIDADES

- **Superintendente:** Deberá aprobar la política y los elementos asociados, facilitar las acciones que el Comité de Gestión de Riesgos y seguridad de la Información apruebe para el adecuado cumplimiento de la presente política.
- **Funcionarios de la Superintendencia:** Deberán cumplir estrictamente lo informado en la presente política.
- **Terceros que cuenten con Acceso a Información:** Deberán cumplir con lo estipulado en la presente política y en los contratos respectivos, cumpliendo las medidas que su contraparte disponga en el cumplimiento de esta.
- **Encargado de Seguridad de la Información:** Deberá desarrollar los procedimientos que especifican roles, responsabilidades, herramientas y tareas para la protección de la información contenida en medios de almacenamiento.
- **Administrador del Contrato:** Deberá hacerse responsable de la coordinación con el proveedor, durante toda la vigencia del contrato.
- **Comité de Gestión de Riesgo y Seguridad de la Información:** Deberá evaluar y, en su caso, aprobar los cambios sugeridos a la presente política por el encargado de seguridad.

G. DE LA POLÍTICA

i. **De la Relación de los Funcionarios con los fiscalizados y/o postulantes a permisos de operación:** Durante el periodo de duración del proceso de otorgamiento de permisos de operación, la relación de los funcionarios de la Superintendencia con los fiscalizados y/o potenciales operadores de casinos de juego, estará regulada por lo establecido en la Circular Interna N°3/2016 que "Establece Protocolo que contiene las instrucciones y órdenes relativas a las formas de comunicación entre los funcionarios de la Superintendencia de Casinos de Juegos y los interesados en el proceso de otorgamiento de permisos de operación de un Casino de Juegos (2016)"

ii. **De la Relación con los Proveedores.**

a. **Revisión de las Condiciones de Seguridad:** Previo a la contratación de cualquier servicio que cuente con acceso a alguno de los activos de la información que tengan un nivel de clasificación de riesgo "Alto", en el inventario de activos institucional, el dueño de éste deberá evaluar los riesgos asociados a los servicios contratados y definir los controles necesarios a implantar si fuese necesario. La evaluación de riesgos debe considerar tanto los aspectos tecnológicos como los relativos a acceso físico de personal externo a las instalaciones de la institución.

b. Contrato del Servicio

- Todos los acuerdos de prestación de servicios deberán quedar formalmente establecidos en un contrato.
- Los contratos de prestación de servicios externos, deben considerar los requerimientos de seguridad para los accesos, procesamiento, comunicación o administración de la información de la organización o la incorporación de productos o facilidades de servicio de procesamiento de información y especificar las condiciones de seguridad que se deben cumplir, por ejemplo, métodos de acceso, usuarios autorizados, responsabilidades legales, etc.
- Los contratos deberán contar con acuerdos de confidencialidad, que resguarden los activos de información de la Superintendencia a los que tendrá acceso el proveedor, en el marco desarrollo del servicio.
- En el caso de no poder materializar el acuerdo de confidencialidad se deberá proponer, que el Comité de Gestión de Riesgos y Seguridad de la Información apruebe e implemente medidas de mitigación, las que deben quedar formalmente documentadas.

c. Control de la prestación del servicio

El Administrador de Contrato encargado de la prestación de un determinado servicio externo es responsable de:

- Verificar periódicamente que el proveedor mantenga las condiciones que le permitan entregar el servicio contratado en los términos acordados.
- Verificar periódicamente que el proveedor externo cumpla con los requisitos de seguridad que se plantearon al servicio.
- Verificar periódicamente que el proveedor externo cumpla con el acuerdo de nivel de servicios (SLA).
- Revisar las actividades que haya realizado el proveedor externo, de modo de detectar cualquier acción que pudiera representar un riesgo para la Superintendencia de Casinos de Juego.

d. Término del contrato

Al finalizar el acuerdo de servicios, el Administrador de Contrato encargado del contrato, será responsable de coordinar la recuperación de los activos y la información que pudiera estar en poder del proveedor y de eliminar los permisos de acceso tanto lógicos como físicos, que se hayan asignado durante la vigencia del contrato.

H. DEL HISTORIAL DE REVISIONES

El historial de revisiones de la política, deberá contener al menos la siguiente información:

a. Versión de la Política
b. Fecha de Revisión
c. Funcionario que Revisa
d. Fecha de aprobación de la Revisión
e. Cambios sugeridos
f. Cambios Aceptados

SCJ | SUPERINTENDENCIA DE CASINOS DE JUEGO

ARTICULO 2°. Publíquese en la web institucional.

ANÓTESE Y NOTIFÍQUESE

DANIEL GARCÍA FERNÁNDEZ
SUPERINTENDENTE DE CASINOS DE JUEGOS (T y P)

DGF/ jmg/gsz/pno
Distribución
- Interesado
- Funcionarios
- Oficina de Partes