SCJ | SUPERINTENDENCIA DE CASINOS DE JUEGO

E12739/2016

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

REF.: APRUEBA POLÍTICA DE CONTROL DE ACCESO LÓGICO A LA INFORMACIÓN DE LA SUPERINTENDENCIA DE CASINOS DE JUEGO.

RESOLUCIÓN EXENTA Nº 558

SANTIAGO, 28 DIC 2016

VISTOS:

Lo dispuesto en la ley Nº 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado; en la Ley 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 los 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, 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

5.- 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 Control de Acceso Lógico a la Información que a continuación se señala:

A. DEL OBJETIVO DE LA POLÍTICA

Esta política establece las definiciones que regulan el acceso a la información que administra la Superintendencia de Casinos de Juego.

B. DEL ALCANCE DE LA POLÍTICA

Todos los funcionarios, funcionarias y terceros, que controlen el acceso a la información de la Superintendencia de Casinos de Juego, considerando procesos de negocios y de apoyo, aplicaciones o sistemas computacionales, software y datos deberán guiar su actuar por la presente política.

C. DEL MARCO REFERENCIAL DE LA POLÍTICA

La presente política dice relación con:

- Inventario Institucional de Activos de Información
- Política General de Seguridad de la Información.

D. DE LA REVISION DE LA POLÍTICA

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.

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.
- **Unidad de Tecnología y Desarrollo de Procesos:** Deberá definir reglas de control de acceso a la información, revocar los accesos de un usuario ante un cambio de cargo o una desvinculación y definir una red segura para el acceso a las aplicaciones que requieren restricción especial de acceso.
- **Propietario de la información:** Canalizar requerimientos de acceso lógico a la información y aprobar el acceso a los datos por parte de los requirentes.
- **Encargado de Seguridad de la Información:** Deberá aprobar las excepciones a las reglas de acceso definidas y recibir y canalizar los informes de contravenciones a la 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.
- **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. Acceso y negación del mismo

a. Los accesos de los usuarios deben ser determinadas en función de las tareas asignadas por la Superintendencia de Casinos de Juego.
b. En ausencia de necesidades u otros argumentos que justifiquen el acceso a la información, este acceso debe ser impedido.

ii. De los Niveles de control de acceso

a. El control de acceso debe ser administrado considerando las distintas instancias que un usuario debe tener para acceder a la información, esto es: redes, sistemas operativos, aplicaciones y bases de datos.
b. En presencia de diferentes rutas para acceder a la información, debe existir consistencia en las medidas de protección en los distintos niveles en que se materializa dicho control de acceso.

iii. De la Administración de los accesos

a. El propietario de la información es quien decide y asigna el acceso a las aplicaciones y los datos.
b. Las decisiones de control de acceso que se tomen, deben ser consistentes con la clasificación de la información definida.
c. Para facilitar la administración de los accesos, se deben definir perfiles de acceso asignables a grupos de usuarios que, por sus responsabilidades en la Superintendencia de Casinos de Juego, presenten necesidades de acceso equivalentes.

iv. De la Segregación de Responsabilidades

a. El otorgamiento de accesos respecto a recursos de información de la Superintendencia de Casinos de Juego, debe considerar una adecuada segregación de funciones, de modo que un mismo empleado no pueda disponer, por su sola voluntad, del control total de un proceso de la superintendencia.
b. Las excepciones a la regla anteriormente descrita, deben ser autorizadas por el Encargado de Seguridad de la Información y debe ser definida respecto de usuarios individuales, de forma que las acciones ejercidas con los accesos otorgados, guarden directa relación con sus funciones y responsabilidades.

v. De las Aplicaciones utilizadas

a. El acceso a las aplicaciones definidas como "aplicaciones seguras" será solamente desde una red segura, instalada para estos efectos.
b. La Unidad de Tecnología y Desarrollo de Procesos debe implementar y mantener una red segura, a la cual solamente puedan conectarse los usuarios debidamente autorizados, y que no permita acceso de otros usuarios, sistemas, programas o utilitarios desde las otras redes de la Superintendencia de Casinos de Juego.

vi. De la Revocación de los Accesos

a. En caso de cambio de cargo de un funcionario, se deben revisar sus permisos de acceso lógico asignados y verificar que éstos sigan siendo válidos de acuerdo a su nueva función.

b. Cuando un funcionario termina su relación laboral con la Superintendencia de Casinos de Juego, sus permisos de acceso a la información deben ser revocados.
c. Las nóminas de funcionarios autorizados y sus respectivos permisos de acceso a la información, deben ser periódicamente revisados.

vii. De la Auditoría de los Accesos: Periódicamente la Unidad de Tecnología y Desarrollo de Procesos, debe revisar los perfiles de acceso definidos y verificar si ellos han sido asignados a los cargos y, por ende, a los usuarios que corresponde.

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

ARTICULO 2°. Publíquese en la web institucional.

ANÓTESE Y NOTIFÍQUESE

SUPERINTENDENCIA DE CASINOS DE JUEGO
SUPERINTENDENTE

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

Superintendencia Jefe Gabinete

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