APRUEBA POLITICA GENERAL DE SEGURIDAD DE LA INFORMACION DEL INSTITUTO NACIONAL DE DEPORTES DE CHILE.

RESOLUCIÓN EXENTA N° 2760

SANTIAGO, 30 AGO. 2019

VISTOS:

a) La Constitución Política de la República.
b) La Ley Nº 19.712, del Deporte.
c) La Ley Nº 18.575 Orgánica Constitucional sobre Bases Generales de la Administración del Estado.
d) La Ley Nº 19.880.
e) Las Resoluciones 7 y 8, de 2019, de la Contraloría General de la República.
f) El Decreto Exento N°120891/57/2019, del 19 de agosto de 2019, del Ministerio del Deporte.
g) El Instructivo Presidencial N°8, de 2018.
h) El Acta de aprobación de la Política de Seguridad, del 16.05.2019 del Comité de Seguridad de la Información del IND.
i) El Memorándum N°110, de 2019, del Departamento de Informática del IND nivel central.

CONSIDERANDO

1. Que el Instituto Nacional de Deportes de Chile, IND, es un servicio público funcionalmente descentralizado, con personalidad jurídica y patrimonio propio, creado por la Ley Nº 19.712, que tiene por objeto ejecutar la política nacional de deportes, así como la promoción de la cultura deportiva en la población, la asignación de recursos para el desarrollo del deporte, y el fomento de la modernización y el desarrollo de la infraestructura deportiva nacional, así como la gestión eficiente de la capacidad instalada, para lo cual podrá ejecutar las acciones y ejercer las facultades que sean necesarias en el cumplimiento de los fines que la ley le asigna.

2. Que, la información que genera y gestiona el Instituto a través de las plataformas y sistemas que hacen uso de tecnología de la información, constituye un activo estratégico clave para asegurar la continuidad de los servicios que brinda y el ejercicio de las funciones y facultades encomendadas por la ley, razón por la cual resulta de la mayor importancia asegurar su integridad y confidencialidad, así como su disponibilidad permanente.

3. Que, con dicho objeto, el Departamento de Informática de este Instituto, en su carácter de unidad técnica especializada en la materia, ha elaborado la Política General de Seguridad de la Información, por la cual habrá de guiarse la ejecución de las labores por todos quienes trabajan en el IND, en cualquier nivel jerárquico y calidad jurídica de contratación, ya sean funcionarios de planta, contratados a honorarios o bajo el Código del Trabajo, o en cualquier calidad que se desempeñen o cumplan funciones dentro de las áreas y departamentos de la institución, así como los proveedores, terceros autorizados o cualquiera que use o tenga acceso a los activos de información de la Institución, entendiéndose por estos a todos los elementos relevantes en la producción, emisión, almacenamiento, comunicación, visualización, recuperación y destrucción de información de valor para el IND.

4. Que, el Comité de Seguridad de la Información aprobó la política referida según acta del 16 de mayo de 2019, procediendo, en consecuencia, su aprobación por acto administrativo formal, otorgándole reconocimiento legal y vinculante para todos los que desempeñen funciones y/o labores en el Instituto Nacional de Deporte de Chile.

RESUELVO:

1° **APRUÉBASE** la Política General de Seguridad de la Información, cuyo texto se inserta a continuación:

1. Declaración Institucional

El Instituto Nacional de Deportes de Chile (IND), es un servicio público funcionalmente descentralizado, con personalidad jurídica y patrimonio propio, creado por la Ley del Deporte N° 19.712 y que tiene por objeto ejecutar la política nacional de deportes, así como la promoción de la cultura deportiva en la población, la asignación de recursos para el desarrollo del deporte y la supervigilancia de las organizaciones deportivas en los términos que establece la ley.

El Instituto reconoce la importancia de la información y de los sistemas de información, así como la necesidad de su protección, por constituir un activo estratégico esencial hasta el punto de poder llegar a poner en peligro la continuidad de la institución, o al menos suponer pérdidas muy importantes si se produjera un daño irreversible de determinados activos de información, así como dar cumplimiento a la legislación chilena vigente en lo que atañe a los datos de carácter institucional y personal, en defensa de los intereses de los usuarios, la institución y otros posibles afectados.

El Instituto protegerá los recursos de información y la tecnología usada para su procesamiento de las amenazas internas o externas, deliberadas o accidentales, con la finalidad de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información. Además de poder garantizar la continuidad de los sistemas de información, minimizar riesgos de daño y asegurar el eficiente cumplimiento de sus objetos estratégicos.

El Instituto considera como activos de información a todos los elementos relevantes en la producción, emisión, almacenamiento, comunicación, visualización, recuperación y destrucción de información de valor para el IND.

Se reconoce que la información que genera y gestiona el Instituto constituye un activo estratégico clave para asegurar la continuidad del servicio. En este contexto, la Política General de Seguridad de la Información está orientada a proteger la información en la totalidad de su ciclo de vida (creación, registro, difusión, modificación, almacenamiento, preservación y eliminación), los medios que permiten dicho ciclo, su acceso y manipulación. Lo anterior, con el fin de garantizar su integridad, disponibilidad y confidencialidad.

Este documento ha sido elaborado en base a la legislación vigente de la República de Chile, entre las que se encuentran el Decreto Supremos N° 83 y además normas que involucran aspectos relacionados con la seguridad de la información.

El incumplimiento de la normativa de seguridad de la información contenida en esta política general constituirá una infracción a los deberes y obligaciones de los/as usuarios/as y podrá dar lugar a la aplicación de sanciones administrativas, previa instrucción del correspondiente procedimiento disciplinario, de conformidad a las normas contenida en la Ley N° 18.834, sobre Estatuto Administrativo.

2. Objetivo

El objetivo de la presente Política General es proporcionar orientación y apoyo a la Dirección Nacional del IND para la seguridad de la información, de acuerdo con los requisitos de la institución y con las regulaciones y leyes pertinentes.

Los objetivos del Sistema de Gestión de Seguridad de la Información son:

- Gestionar los riesgos de seguridad de la información de los activos vinculados a los procesos de provisión de Productos Estratégicos (bienes y servicios), basado en la norma NCh-ISO 27001:2013 con foco en Ciberseguridad, asegurando la continuidad de los servicios críticos de la Institución para lograr conservar la confidencialidad, integridad y disponibilidad de la información.
- Contar con una visión global sobre el estado de los activos de información institucionales, las medidas de seguridad que se están aplicando y los resultados que se están obteniendo de dicha aplicación.
- Capacitar y sensibilizar a los funcionarios en temas de seguridad de la información.

3. Alcance o amplitud de la política

El alcance del Sistema de Gestión de Seguridad de la Información está determinado por los procesos que dan soporte a los productos estratégicos del IND, definidos en la Ficha de Definiciones Estratégicas vigente.

Esta Política General de Seguridad de la Información debe ser conocida y aplicada por todos quienes trabajan en el IND, en cualquier nivel jerárquico, ya sean funcionarios de planta, contratados asimilados a grados, honorarios o en cualquier calidad que se desempeñen, que laboren o cumplan funciones dentro de las áreas y departamentos de la institución, así como los proveedores, terceros autorizados o cualquiera que use o tenga acceso a los activos de información de la Institución.

4. Roles y responsabilidades

a) **Alta Dirección:** La Alta Dirección del IND es responsable de desplegar los medios técnicos, económicos y humanos necesarios para garantizar la correcta implementación del SGSI.

b) **Comité de Seguridad de la información:** El Comité de Seguridad de la Información es designado mediante Resolución Exenta de la Dirección Nacional del Instituto, y tiene como responsabilidad principal revisar y proponer al Director Nacional los ajustes necesarios a la presente Política General de Seguridad de la Información y aprobar la normativa y planes de trabajo derivados de la implementación de la misma.

c) **Encargado/a de Seguridad:** Debe coordinar todas las actividades en esta materia dentro del IND. El/la Encargado/a de Seguridad es designado mediante Resolución Exenta de la Dirección Nacional del Instituto, dónde se establecen las funciones y responsabilidades que debe asumir en este ámbito.

d) **Propietario o dueño de proceso:** Es el responsable del proceso y de la información asociada. Su nivel jerárquico puede estar ligado a la responsabilidad de una Dirección, Departamento o Unidad. Es quien determina el acceso a los distintos activos de información de su área de trabajo y quien autoriza sus distintos usos.

e) **Funcionarios/as:** Deben cumplir toda la normativa existente en materia de seguridad de la información y reportar oportunamente los incidentes y/o debilidades de seguridad de la información que detecten, utilizando los canales y herramientas que para este efecto pone a disposición el IND.

5. Definiciones

- **IND o Instituto:** Instituto Nacional de Deportes.
- **Funcionarios/as:** Toda persona que tenga un vínculo laboral con el Instituto Nacional de Deportes.
- **Usuarios:** Personal de la institución que utiliza el equipamiento informático, software e infraestructura de red institucional o algún activo de información.
- **Activos de Información:** Corresponden a todos aquellos elementos relevantes en la producción, emisión, almacenamiento, comunicación, visualización y recuperación de información de valor para la institución. De esta forma podemos distinguir 3 niveles básicos de activos de información:
  - La Información propiamente tal, en sus múltiples formatos (papel, digital, texto, imagen, audio, video, etc.)
  - Los Equipos/Sistemas/infraestructura que soportan esta información
  - Las Personas que utilizan la información, y que tienen el conocimiento de los procesos institucionales.

- **Seguridad de la información:** Todas aquellas medidas preventivas y reactivas que permitan resguardar y proteger los activos de información, buscando mantener la confidencialidad, integridad y disponibilidad de los mismos.
- **Ciberseguridad:** Conjunto de herramientas, políticas, métodos de gestión de riesgos, prácticas y tecnologías que pueden utilizarse para proteger los activos de información de la organización y sus usuarios en el entorno digital, buscando garantizar la disponibilidad, integridad y confidencialidad de la información.
- **Comité de Seguridad de la Información (CSI):** El Comité de Seguridad de la Información (CSI), es un cuerpo integrado por representantes de todas las áreas sustantivas del Organismo, destinado a garantizar el apoyo manifiesto de las autoridades a las iniciativas de seguridad.
- **Encargado de Seguridad de la Información:** Es la persona que cumple la función de supervisar el cumplimiento de la presente Política y de asesorar en materia de seguridad de la información al Jefe Superior del Servicio y a los integrantes del Organismos que así lo requieran.
- **Confidencialidad:** Es la propiedad de la información por la que se garantiza que es accesible sólo para aquellas personas debidamente autorizadas.
- **Integridad:** Es la propiedad de la información que busca salvaguardar la precisión y completitud de la información y los métodos de procesamiento.
- **Disponibilidad:** Es la capacidad de asegurar que las personas autorizadas tengan acceso a la información y bienes asociados cuando lo requieran.
- **Alta Dirección:** Constituido por el/la directora/a Nacional, Directores/as Regional, Jefaturas de División de Administración y Finanzas, Desarrollo y Actividad Física y Deportes.

- **Incidente:** Está indicado por uno o múltiples eventos no esperados. Esto tiene una alta probabilidad de comprometer la continuidad de las operaciones del negocio. Se puede definir como un incidente de seguridad de la información al acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de activos de información; un impedimento en la operación normal de las redes, sistemas o recursos informáticos; o una violación a la Normativa de Seguridad de la Información del Servicio.
- **Amenaza:** Evento generado a partir de un agente externo o interno de la institución, que tenga el potencial de generar algún grado de daño (ya sea en relación a la confidencialidad, integridad o disponibilidad) en uno o más activos de información institucional.
- **Vulnerabilidad:** Se refiere a alguna condición de debilidad o fragilidad que se encuentra presente en el activo identificado. Usualmente se traduce en una debilidad o ausencia de control, que posibilita la ocurrencia de un incidente y que pueden afectar a uno o más activos de información.

6. Marco general para la normativa interna de Seguridad de la Información.

- Formato de las políticas y procedimientos

Las políticas de seguridad y los procedimientos asociados son establecidos por el IND, conforme a los formatos desarrollados y vigentes establecidos. Cada documento generado debe contener como mínimo los siguientes puntos:

Políticas	Procedimientos
o Portada: ▪ Nombre de la política ▪ Número última versión ▪ Fecha última versión ▪ Código de documento o Objetivo. o Alcance. o Documentos Relacionados o Materias específicas que aborda o Roles y Responsabilidades. o Difusión de la política. o Revisión de la política. o Definiciones. o Desarrollo de la política. o Cuadro firma de aprobaciones o Control de versiones.	o Portada: ▪ Nombre del procedimiento ▪ Código de documento ▪ Controles ISO27002 ▪ Fecha última versión ▪ Número última versión o Objetivo. o Alcance. o Responsabilidades. o Detalle de actividades. o Glosario de términos. o Registros de operación o Cuadro firma de aprobaciones o Control de versiones.

- Aprobación de la normativa

La normativa debe ser revisada y aprobada por el Comité de Seguridad de la Información y por el/la Encargado/a de Seguridad de la Información, lo cual debe quedar registrado en las actas de reunión de CSI.

En particular, esta Política General de Seguridad de la Información debe ser aprobada por el Jefe del Servicio a través de una Resolución Exenta.

- Difusión de las Políticas

Una vez aprobada la política de seguridad de la información, esta debe ser difundida a todos los funcionarios del IND, para su correcta aplicación. La forma de difusión será a través de la publicación de las políticas, procedimientos e instructivos en la intranet institucional o cualquier otro mecanismo que se estime pertinente, lo que será notificado mediante correo electrónico.

- Revisión de las Políticas

Las políticas de seguridad de la información deben ser analizadas cada dos años o o ante cualquier cambio significativo de tecnología, personal o evento que amerite su reevaluación para asegurar su continuidad, idoneidad, eficiencia y efectividad; en cualquier caso estas revisiones se realizaran en las reuniones del CSI. Los ajustes a las políticas deben ser solicitados al CSI y serán presentados a el/la Encargado/a de Seguridad de la Información del Instituto.

Se deberá, asimismo, programar, por lo menos una vez al año, la revisión de cumplimiento y la efectividad del Sistema de Gestión de Seguridad de la Información. En esa oportunidad se deberán revisar los incidentes ocurridos a la fecha y proponer planes de mejora en los casos que sea necesario.

7. Sanciones.

Toda infracción a esta política así como cualquier denuncia referida a funcionarios del IND podrá ser investigado y/o denunciado ante la jefatura correspondiente, debiéndose aplicar las sanciones administrativas que procedan, de acuerdo al D.F.L. N°29, de 2004, del Ministerio de Hacienda, que fija el texto refundido, coordinado y sistematizado de la Ley 18.834 sobre Estatuto Administrativo y ejercer las acciones civiles y penales que correspondan, conforme a la magnitud y características del incumplimiento de ésta.

8. Control de versiones

Versión	Fecha	Responsable	Descripción
Versión 1	14-12-2011	Cristian Villalobos Z.	Se elabora esta primera versión del presente documento para dar cumplimento al PMG-SSI 2011 y abordar requerimientos internos del IND.
Versión 2	04-08-2016	Cristian Villalobos Z.	Se ajusta el formato de la política de acuerdo a los requisitos de la red de expertos
Versión 3	10-07-2018	Cristian Villalobos Z.	Revisión bianual de la política por el CSI. - Se incorpora el cuadro de formato de la normativa. - Se agrega el capítulo de sanciones. - Se modifica la difusión.
Versión 4	16-05-2019	Cristian Villalobos Z.	- Se incorpora el concepto de Ciberseguridad en el objetivo y definiciones. - Se detallan parte de las responsabilidades del CSI.

2° **PÓNGASE**, la presente resolución aprobatoria de la Política General de Seguridad de la Información, en conocimiento de todos los funcionarios y trabajadores del Servicio mediante su publicación en la intranet institucional.

3° **PUBLÍQUESE** la presente Resolución Exenta en el banner de Internet Gobierno Transparente del Sitio Web del Instituto Nacional de Deportes de Chile.

ANÓTESE, COMUNÍQUESE Y ARCHÍVESE.

INSTITUTO NACIONAL DE DEPORTES DE CHILE
DIRECTORA NACIONAL (S)
IND

SOFIA RENGIFO OTTONE
DIRECTORA (S) NACIONAL
INSTITUTO NACIONAL DE DEPORTES DE CHILE

JBB / ICL / CMC / OCC / PAO
Folio: 1721
DISTRIBUCIÓN:
- Gabinete Dirección Nacional.
- División de Administración y Finanzas.
- Departamento de Informática.
- Departamento de Comunicaciones.
- Unidad de Planificación y Control de Gestión.
- Unidad de Transparencia.
- Oficina de Partes