APRUEBA NORMAS DE INTEGRACIÓN Y FUNCIONAMIENTO DEL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD DEL INSTITUTO NACIONAL DE DEPORTES DE CHILE.

_____

RESOLUCIÓN EXENTA N° **NC-02057/2022**

SANTIAGO, **miércoles, 17 de agosto de 2022**

VISTOS:

a) La Constitución Política de la República.
b) El D.F.L. Nº 1/19.563, de 2000, que fijó el Texto refundido, coordinado y sistematizado de la Ley Nº 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado.
c) La Ley N° 19.712, del Deporte.
d) La Ley N° 19.880, que establece las Bases de los Procedimientos Administrativos que rigen los Actos de los Órganos de la Administración del Estado;
e) El Decreto Supremo N° 83, de 2005, del Ministerio Secretaria General de la Presidencia;
f) El Decreto Exento N° 120891/19/2022, de 28 de abril de 2022, de la Subsecretaria de Deportes;
g) Resolución Exenta N° 1535, de 2009, del Ministerio de Economía, Fomento y Reconstrucción;
h) La Resolución Exenta N° 1898, de 28 de septiembre de 2020, que detalla la composición y normativa del Comité de Seguridad de la Información del Instituto Nacional de Deportes;
i) La Resolución N°7 de 2019, de la Contraloría General de la República, que fija normas sobre exención del trámite de Toma de Razón;
j) El Memorándum N° NC-941/2022, de 02 de mayo de 2022, de la Jefa (S) del Departamento de Informática.

CONSIDERANDO:

1. Que, el Instituto Nacional de Deportes de Chile, conforme lo dispuesto en el artículo 10, de la Ley N° 19.712, del Deporte, es un servicio público funcionalmente descentralizado, dotado de personalidad jurídica y patrimonio propio, que se vincula con el Presidente de la república a través del Ministerio del Deporte.

2. Que, la Ley N° 19.799, sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma, regula los documentos electrónicos y sus efectos legales, la utilización en ellos de firma electrónica, la prestación de servicios de certificación de estas firmas y el procedimiento de acreditación al que podrán sujetarse los prestadores de dicho servicio de certificación, con el objeto de garantizar la seguridad en su uso, definiendo en su artículo 2° el documento electrónico como toda representación de un hecho, imagen o idea que sea creada, enviada, comunicada o recibida por medios electrónicos y almacenada de un modo idóneo para permitir su uso posterior.

3. Que, de acuerdo al artículo 11, del Decreto N° 83, de 2005, del Ministerio Secretaria General de la Presidencia, que aprueba la Norma Técnica para Órganos de la Administración del Estado sobre Seguridad y Confidencialidad de los documentos electrónicos, los órganos de la administración regidos por dicha norma deben establecer una política que fije las directrices

generales que orienten la seguridad de la información dentro de cada institución, que refleje claramente el compromiso, apoyo e interés en el fomento y desarrollo de una cultura de seguridad institucional.

4. Que, mediante Resolución Exenta N° 1738, de 28 de 2020, la Dirección Nacional del Instituto Nacional, se designó al Encargado de Seguridad de la Información del Instituto Nacional de Deportes de Chile, en cumplimiento del artículo 12 del referido Decreto N° 83, de 2005.

5. Que, es necesario que el Servicio, continuamente, gestione adecuadamente la Seguridad de la Información y la Ciberseguridad, con el objeto de mejorar los niveles de protección de los activos de información relevantes que dan sustento a sus procesos estratégicos y de soporte.

6. Que, en virtud de la Resolución Exenta N° 1535, de 2009, del Ministerio de Economía, Fomento y Reconstrucción, se declaró Norma Oficial de la República de Chile a la norma NCh-ISO 27002, sobre Tecnología de la Información – Código de Prácticas para la gestión de la Seguridad de la información-, la cual dispone, entre otras normas, que las actividades referentes a la Seguridad de la Información deben ser coordinadas por representantes de diferentes partes de la organización con funciones y roles pertinentes.

7. Que, para el cumplimiento de tales objetivos, se creó el Comité de Seguridad de la Información y Ciberseguridad, que, en función del marco legal y tecnológico vigente, proponga al Jefe del Servicio la Política de Seguridad de la Información, la implemente, desarrolle, mantenga y mejore en el tiempo.

8. Que, en virtud del Instructivo Presidencial N° 008, de 23 de octubre de 2018, se impartieron instrucciones urgentes en materia de Ciberseguridad, para la protección de redes, plataformas y sistemas informáticos de los órganos de la Administración del Estado, entre las cuales se instruye la designación de un encargado de Ciberseguridad de alto nivel en cada servicio.

RESUELVO:

1. APRUÉBANSE las normas para la creación, integración y funcionamiento del Comité de Seguridad de la Información y Ciberseguridad, en el Instituto Nacional de Deportes, cuyo texto es del siguiente tenor:

NORMAS DE INTEGRACIÓN Y FUNCIONAMIENTO DEL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD DEL INSTITUTO NACIONAL DE DEPORTES

ARTÍCULO 1°: Créase el Comité de Seguridad de la Información y Ciberseguridad del Instituto Nacional de Deportes de Chile, en adelante CSI y CS, respectivamente, el que estará conformado por el/la Encargado/a de Seguridad de la Información, quien lo presidirá, y por las personas que desempeñan las funciones que a continuación se indican, o quién éstas designen en su representación, las que actuarán con las mismas facultades del/la Titular, esto es, con derecho a voz y a voto para los acuerdos y/o decisiones que se adopten en cumplimiento de su cometido.

- Encargado/a de Seguridad de la Información
- Encargado/a de Ciberseguridad
- Jefatura del Departamento de Informática
- Jefatura Unidad de Planificación y Control de Gestión.

- Encargado de Riesgo
- Jefatura de Departamento Jurídico
- Representante del Departamento de Comunicaciones
- Encargado/a del Área de Operaciones del Departamento de Informática.
- Encargado/a PMG de Seguridad de la Información.

En las sesiones del Comité de Seguridad de la Información y Ciberseguridad, podrá participar un/a representante de la Unidad de Auditoría Interna, el/la que tendrá sólo derecho a voz.

El Comité de Seguridad de la Información y Ciberseguridad designará entre sus integrantes a un Secretario/a, quién tendrá por función llevar y custodiar un registro de las actas de las reuniones del CSI y CS, ya sean estas programadas o extraordinarias, con su respectivo control de asistencia. El/la Encargado/a de Seguridad de la Información velará por la mantención actualizada de estos registros.

En los casos en que el/la Secretario/a designado/a no asistiere a una reunión de CSI y CS, se designará un/a reemplazante dentro de los/as participantes de dicha reunión, quien deberá efectuar el registro del acta correspondiente consignando en la misma la asistencia de sus miembros con indicación de la calidad en que asiste, sea este/a de titular o reemplazante.

ARTÍCULO 2°: Los/as reemplazantes o suplentes podrán asistir a las sesiones del CSI y CS conjuntamente con su respectivo/a titular, circunstancia en la que aquellos sólo tendrán derecho a voz.

ARTÍCULO 3°: El quórum para sesionar y adoptar válidamente acuerdos será de a lo menos cinco de sus integrantes. Sus acuerdos se adoptarán por mayoría simple de votos. En caso de empate dirimirá el Encargado/a de Seguridad de la Información del IND.

ARTÍCULO 4°: En todo lo demás, el Comité de Seguridad de la Información y Ciberseguridad podrá definir su forma de funcionamiento y normas que estime necesarias para su operación, dejando constancia de ello en el acta de la sesión donde se arribe a dicho acuerdo, procurando que dicho acuerdo no infrinja la normativa que regula la materia.

ARTÍCULO 5°: Los/as funcionarios/as del Instituto Nacional de Deportes, con independencia de sus cargos, estamentos y/o funciones, deberán cumplir a cabalidad las políticas y normas en materia de Seguridad de la Información y Ciberseguridad.

ARTÍCULO 6°: El CSI y CS contará entre sus facultades el poder requerir información con respecto de un hecho relacionado con la Seguridad de la Información o Ciberseguridad a cualquier funcionario/a o prestador de servicios del IND.

Este derecho reconocerá como límites la exhibición de información contenida en archivos o documentos electrónicos cuya exhibición se encuentre limitada, restringida o prohibida, como aquella de carácter reservado, o cuya exhibición pueda afectar a terceros, o que se refiera a información de carácter sensible, entre otras. En todos estos casos, para acceder a dicha información, se deberá cumplir con todos aquellos requisitos establecidos en la legislación y reglamentos pertinentes, de forma previa a su entrega.

ARTÍCULO 7°: El Comité de Seguridad de la Información y Ciberseguridad, cuando lo estime conveniente, podrá invitar a terceros a sus reuniones, los/as cuales podrán aportar su juicio experto, pero sólo con derecho a voz.

ARTÍCULO 8°: El Comité de Seguridad de la Información y Ciberseguridad deberá revisar, actualizar y elaborar Políticas y Procedimientos en materias de la Seguridad de la Información y Ciberseguridad.

ARTÍCULO 9°: Los roles, funciones y atribuciones de base para el funcionamiento del Sistema de Gestión de Seguridad de la Información (SGSI), se definen en el siguiente cuadro:

Responsabilidad en la administración de la SI y CS	Roles claves	Funciones y atribuciones
Director/a Nacional	Impulsar la implementación y mejora del SGSI	• Aprobar la Política General de Seguridad de la Información y validar el proceso del SGSI. • Aprobar las estrategias y mecanismos de control para el tratamiento de riesgos que afecten a los activos de información institucionales.
Comité de Seguridad de la Información y Ciberseguridad	Gestionar e implementar la Política de General de Seguridad de la Información y de Ciberseguridad del IND.	• Revisar y proponer al/la Directora/a Nacional, los ajustes necesarios a la Política General de Seguridad de la Información y Ciberseguridad. • Aprobar las políticas específicas de seguridad y los planes de trabajo, derivados de la implementación de la Política General de Seguridad de la Información. • Supervisar la implementación de procedimientos y estándares que se desprenden de las políticas de seguridad. • Proponer estrategias e iniciativas específicas para la implementación de los controles necesarios para la elaboración de las políticas de seguridad y la debida solución y/o mitigación de las situaciones de riesgo detectadas. • Mediar en conflictos que se pudieran detectar relacionados con la seguridad de la información y Ciberseguridad y los riesgos asociados y proponer soluciones. • Mantener una coordinación permanente con el Comité de Riesgos del IND, para el alineamiento e impulsar estrategias comunes. • Gestionar los incidentes de seguridad de la información y Ciberseguridad detectados, a fin de establecer acciones preventivas y correctivas. • Reportar a la Dirección Nacional, respecto a oportunidades de mejora en el SGSI, así como de los incidentes relevantes y su solución.

Encargado/a de Seguridad de la Información	Coordinación de actividades de la gestión en la Seguridad de la Información y Ciberseguridad	• Tener a su cargo la elaboración de las políticas de seguridad al interior del IND, el control de su implementación y velar por su correcta aplicación. • Coordinar actividades de los Comités de Seguridad de la Información y Ciberseguridad. • Gestionar la debida respuesta y priorización al tratamiento de incidentes y riesgos vinculados a los activos de información de los procesos institucionales y sus objetivos de negocio. • Monitorear el avance general de la implementación de las estrategias de control y tratamiento de riesgos vinculados al SGSI. • Mantener comunicación con otras unidades del IND para apoyar los objetivos de seguridad. • Establecer comunicación permanente con Encargados/as de Seguridad de otros servicios públicos y especialistas externos que le permitan estar al tanto de las tendencias, normas y métodos de seguridad pertinentes.
Encargado de Ciberseguridad	Mantener una comunicación constante y efectiva con el Equipo de Respuesta (CSIRT) del Ministerio del Interior y Seguridad Pública ante Incidentes de Seguridad Informática.	• Reducir la exposición del IND a las amenazas de Ciberseguridad. • Liderar los planes de pruebas de seguridad. • Evaluar la efectividad de los controles implementados. • Reportar al Encargado/a de Seguridad de la Información las alertas de seguridad notificadas por el CSIRT para su oportuno tratamiento. • Informar al CSIRT el estado de avance de una alerta de seguridad reportada, así mismo, informar cuando está alerta sea solucionada para el cierre del ticket por parte del CSIRT.

ARTÍCULO 10°: Las normas precedentes entraran en vigor a contar de la fecha de emisión del acto administrativo que las apruebe.

2. DÉJASE SIN EFECTO la Resolución Exenta N° 1898, de 28 de septiembre de 2020, del IND, archivándose un ejemplar del presente acto administrativo de manera conjunta con la citada resolución.

3. PUBLÍQUESE la presente Resolución Exenta en el banner de Gobierno Transparente de la página web del Instituto Nacional de Deportes: www.ind.cl

ANÓTESE, COMUNÍQUESE Y ARCHÍVESE

ISRAEL FERNANDO CASTRO LOPEZ
DIRECTOR NACIONAL (S)
INSTITUTO NACIONAL DE DEPORTES DE CHILE

OPV/MMO/CBM/LCC/CMC/CVZ

DISTRIBUCIÓN:

- Gabinete Dirección Nacional
- División de Administración y Finanzas
- Departamento de Informática
- Archivo Departamento Jurídico
- Unidad de Transparencia, Lobby y Participación Ciudadana
- Subcomité de Gestión de Seguridad y Confidencialidad del Documento electrónico y activos de la información del Ministerio del Interior
- Unidad de Gestión, Desarrollo y Relaciones Laborales
- Departamento de Gestión y Desarrollo de las Personas
- Unidad de Planificación y Control de Gestión
- Direcciones Regionales
- Oficina de Partes