APRUEBA POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO NACIONAL DE DEPORTES DE CHILE.

RESOLUCIÓN EXENTA N° **NC-01925/2022**

SANTIAGO, **viernes, 29 de julio 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, del Ministerio del Deporte;
g) Resolución Exenta N° 1535, de 2009, del Ministerio de Economía, Fomento y Reconstrucción;
h) La Política General de Seguridad de la Información del Instituto Nacional de Deportes, aprobada mediante Resolución Exenta N° 2760, de 30 de agosto de 2019;
i) 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;
j) La Resolución N°7 de 2019, de la Contraloría General de la República, que fija normas sobre exención del trámite de Toma de Razón;
k) El Memorándum N° NC-941/2022, de 02 de mayo de 2022, de la Jefa (S) del Departamento de Informática.
l) Política General de Seguridad de la Información, aprobada con fecha 27 de julio de 2022;

CONSIDERANDO:

1. Que el Instituto Nacional de Deportes de Chile, es un servicio público funcionalmente descentralizado, con personalidad jurídica y patrimonio propio, creado por la Ley N°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, se emitió por parte de esta Institución la Resolución Exenta N°2760, de 30 de agosto de 2019, que contiene la actual Política General de Seguridad de la Información.

4. Que, para asegurar el resguardo de la información, y con el propósito de actualizar la normativa vigente a las nuevas exigencias en esta materia, el Departamento de Informática de este Instituto, en su carácter de unidad técnica especializada en la materia, ha elaborado una nueva 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.

5. Que, la nueva política referida en los considerandos previos fue aprobada con fecha 27 de julio de 2022, en su versión final, 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 POLITICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN , del Instituto Nacional de Deportes de Chile, cuyo texto se inserta a continuación:

POLITICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN
Sistema de Gestión de Seguridad de la Información

Versión: 5
Fecha Aprobación: 27-07-2022
Código: IND-SSI-A05-POL-05

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 seguridad de la información y de los sistemas de información, así como la necesidad de protección, por constituir un activo estratégico esencial hasta el punto de llegar a poner en peligro la continuidad operativa 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/as usuarios/as, 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 operativa de los sistemas de información, minimizar riesgos de daño y asegurar el eficiente cumplimiento de sus objetivos 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 Supremo 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 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.

- Difundir y sensibilizar a los funcionarios en temas de vinculados a la seguridad de la información.

3. ALCANCE 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 las Definiciones Estratégicas vigente (Formulario A1, disponible en la intranet institucional https://intranet.ind.cl/wp-content/uploads/2021/09/F-A1-2019-2022.pdf).

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 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

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

Comité de Seguridad de la Información: es designado mediante Resolución Exenta de la Dirección Nacional del IND, y tiene como responsabilidad principal revisar y proponer a la Alta Dirección 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.

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

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.

Funcionarios/as: Conocer y cumplir la Política General de Seguridad de la información, como la normativa que se desprende de ella.
Utilizar adecuadamente los activos de información que la institución ha puesto a su disposición.
Utilizar adecuadamente la plataforma tecnológica, servicios informáticos, equipamiento y dispositivos institucionales.

5. DEFINICIONES

- Instituto o IND: Instituto Nacional de Deportes.
- Funcionarios/as: Toda persona que tenga un vínculo laboral con el Instituto Nacional de Deportes.
- Usuarios/as: Personal de la institución que utiliza el equipamiento informático, software e infraestructura tecnológica institucional o algún otro 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, los sistemas y/o la infraestructura tecnológica 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/as en el entorno digital, buscando garantizar la disponibilidad, integridad y confidencialidad de la información.
- Comité de Seguridad de la Información (CSI): Es un cuerpo integrado por representantes de todas las áreas sustantivas del Instituto, destinado a garantizar el apoyo manifiesto de las autoridades a las iniciativas de seguridad.
- Comité de Ciberseguridad: Es un cuerpo integrado por representantes de todas las áreas sustantivas del instituto, cuya labor es revisar y evaluar el estado de avance de todas la medidas de Ciberseguridad implementadas hasta la fecha en base al Instructivo Presidencial N°8 y de la Política Nacional de Ciberseguridad.
- Encargado/a de Seguridad de la Información (ESI): 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/a de Servicio y a los integrantes del Instituto 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 Director/a Nacional, Directores/as Regionales, Jefaturas de División de Administración y Finanzas, División de Infraestructura y Recintos y División de 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 IND.
- 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. Cada documento generado debe contener como mínimo los siguientes puntos:

POLÍTICAS	PROCEDIMIENTOS
• Portada: o Nombre de la política o Número de la última versión	• Portada: o Nombre del procedimiento o Código del procedimiento

○ Fecha de la última versión ○ Código de documento • Objetivo • Alcance • Documentos Relacionados • Materias específicas que aborda • Roles y responsabilidades • Difusión de la política • Revisión de la política • Definiciones • Desarrollo de la política • Control de versiones • Control de revisiones y aprobaciones	○ Controles ISO27002 ○ Fecha de la última versión ○ Número de la última versión • Objetivo • Alcance • Referencias • Términos y definiciones • Formularios / Formatos Aplicables • Modo de operación • Roles y responsabilidades • Identificación de riesgos • Recursos • Registros • Indicador de gestión • Anexos

- 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 del CSI.

  En particular, esta Política General de Seguridad de la Información debe ser aprobada por el Jefe/a de 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 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 IND.

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

7. RESPONSABILIDAD DE LOS/AS FUNCIONARIOS/AS

Los/as funcionarios/as deben cumplir con las normas relacionadas con la seguridad de la información, todas las cuales se entienden formar parte de la presente política. Su infracción acarreará la responsabilidad administrativa que corresponda a quienes resulten responsables, sin perjuicio de la responsabilidad civil o penal que pueda asistir a los infractores por los mismos hechos.

Las políticas de seguridad de la información que se encuentran vigentes en la Institución son las siguientes:

- Política de la Organización de la Seguridad de la Información.
- Política de Seguridad de Uso de Dispositivos Móviles.
- Política de Uso del Correo Electrónico Institucional.
- Política de la Continuidad de la Seguridad de la Información.
- Política de Cumplimiento.
- Política de Recursos Humanos.
- Política de Administración de Activos de Información.
- Política de Control de Acceso a los Sistemas de Información.
- Política de Seguridad Física y Ambiental.
- Política de Seguridad de las Operaciones.
- Política de Seguridad de las Comunicaciones.
- Política de Desarrollo Seguro.
- Política de Seguridad para las Relaciones con los Proveedores.
- Política de Gestión de Incidentes de Seguridad de la Información.

Son infracciones específicas vinculas a la Seguridad de la Información, además del incumplimiento de las referidas instrucciones, entre otras, las siguientes:

- Eliminación y/o borrado de información cuya conservación es obligatoria para el Servicio, como por ejemplo: informes, contratos, documentos, información financiera, información legal, entre otras.
- Filtrar hacia el exterior del Servicio información que contenga datos sensibles de los funcionarios, o documentos del Servicio que no tengan el carácter de públicos de acuerdo a la normativa vigente.
- Mal uso de los recursos informáticos, afectando la normal operación de la Institución.
- Ingresos no autorizados a los sistemas de información, como por ejemplo, utilizar credenciales ajenas.
- Utilizar el correo electrónico institucional en provecho propio o de terceros para fines ajenos a los institucionales.
- Descargar desde internet contenidos ajenos a los fines de la Institución, como por ejemplo: películas, música, publicidad, entre otras. Excepcionalmente, se podrá acceder a dicho contenido, siempre y cuando sea necesario para el cumplimiento de las funciones de la Institución, lo que se evaluará caso a caso entre el área requirente y el Departamento de Informática.
- Acceder a páginas de internet que no estén autorizadas por la institución.

Aprobaciones, firmas y controles de cambios en documento que se adjunta.

2. NOTIFÍQUESE, la presente resolución aprobatoria de la POLITICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN en conocimiento de todos los funcionarios y trabajadores del Servicio, mediante su difusión por correo electrónico masivo, al cual se adjuntará la presente política.

3. PUBLIQUESE la presente Resolución Exenta, en el banner gobierno transparente de la página web del Instituto Nacional de Deportes de Chile.

ANÓTESE, COMUNÍQUESE Y ARCHÍVESE

ESTE DOCUMENTO CUENTA CON FIRMA ELECTRÓNICA AVANZADA
IND
Instituto Nacional de Deportes

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
- Departamento Jurídico
- Comité de Seguridad de la Información
- Unidad de Partes y Gestión Documental