



POLITICA DE LA ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN SISTEMA DE SEGURIDAD DE LA INFORMACIÓN

Página: Página 1 de 6

Versión : 2.0

Fecha Aprobación : 16 de mayo de 2019

Código: IND-SSI-A06-POL-01

1. OBJETIVO

Establecer un marco de administración para iniciar y controlar la implementación y operación de la Seguridad de la Información dentro del Instituto Nacional de Deportes (IND), a través de un sistema de gestión basado en la norma NCh-ISO 27001:2013, con foco en Ciberseguridad, asegurando la continuidad de los servicios críticos para lograr conservar la confidencialidad, integridad y disponibilidad de la información.

2. ALCANCE

Esta Política aplica para todo el personal que trabaje en o para el IND, ya sean funcionarios de planta, a contrata, a honorarios, regidos por el Código del Trabajo, asesores, consultores, practicantes, y otros trabajadores, incluyendo las empresas que presten servicios para el IND, cuyas funciones dan soporte a los procesos de provisión de Productos Estratégicos consignados en el Formulario de Definiciones Estratégicas (A1).

3. MATERIAS QUE ESPECÍFICAS QUE ABORDA

- A.06.01.01 Roles y responsabilidades de la Seguridad de la Información
- A.06.01.02 Segregación de deberes
- A.06.01.03 Contacto con las autoridades
- A.06.01.04 Contacto con los grupos de interés
- A.06.02.02 Trabajo remoto

4. ROLES Y RESPONSABILIDADES

- Comité de Seguridad de la Información
 - Ser responsable del ciclo de vida de las políticas de Seguridad de la Información en el IND.
 - Velar por el cumplimiento y actualización de la Política General de Seguridad de la Información.
 - Validar, aprobar y difundir, al interior de la institución, las políticas y procedimientos que forman parte de la normativa de Seguridad de la Información del IND.
 - Velar por la correcta implementación de los controles de seguridad en la plataforma tecnológica del IND.



POLITICA DE LA ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN SISTEMA DE SEGURIDAD DE LA INFORMACIÓN

Página: Página 2 de 6

Versión : 2.0

Fecha Aprobación : 16 de mayo de 2019

Código: IND-SSI-A06-POL-01

- Monitorear los incidentes de seguridad que pudieran afectar la seguridad al interior del IND, con el fin de establecer acciones preventivas y correctivas.
- Encargado/a de Seguridad de la Información
 - Asesorar al Jefe de Servicio en materias de Seguridad de la Información.
 - Organizar las actividades del Comité de Seguridad de la Información.
 - Coordinar 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 los riesgos asociados a la Seguridad de la Información.
 - Tener a su cargo el desarrollo inicial de las políticas de seguridad al interior del IND, controlar su implementación y velar por su correcta aplicación.
 - Coordinar la respuesta a incidentes que afecten a los activos de información institucionales.
 - Tomar las acciones necesarias para resguardar y asegurar la continuidad operacional del IND frente a incidentes de seguridad de la información.
 - Mantener coordinación con otras unidades del IND para apoyar los objetivos de seguridad y establecer puntos de enlace con los Encargados de Seguridad de otros organismos públicos y especialistas externos, que le permitan estar al tanto de las tendencias, normas y métodos de seguridad de la información pertinentes.
- Encargado/a de Ciberseguridad
 - Alinear los esfuerzos de las distintas áreas, respecto a la protección de los sistemas tecnológicos y a la información contenida en ellas, según los criterios de Ciberseguridad.
 - Velar por el cumplimiento de la mitigación de riesgos que puedan afectar a la plataforma tecnológica, por parte de TI y Proveedores de Servicios (Comunicaciones, Datacenter, Cloud, Servicios de Seguridad, Firma Electrónica y Certificados Digitales para Sitios Web, Adopción de URL Institucional que incluya “.gob.cl”, entre otros).
 - Gestionar al interior de la institución, todo requerimiento de información solicitado por el Equipo de Ciberseguridad del Ministerio del Interior y Seguridad Pública.
 - Informar al CSIRT sobre cualquier incidencia que pueda afectar a la plataforma tecnológica de la institución, sea ésta que se encuentre expuesta a Internet o que se encuentre en su red interna.



POLITICA DE LA ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN SISTEMA DE SEGURIDAD DE LA INFORMACIÓN

Página: Página 3 de 6

Versión : 2.0

Fecha Aprobación : 16 de mayo de 2019

Código: IND-SSI-A06-POL-01

- Apoyar el proceso de Sensibilización en Materias de Ciberseguridad al interior de la Institución.

5. REVISIÓN Y EVALUACIÓN

La presente Política debe ser objeto de revisión y de evaluación en relación con su correcta aplicación cuando se cumplan dos años de su aprobación, o bien, en forma extraordinaria, cada vez que se presente un evento que propicie un ajuste de las declaraciones establecidas en esta Política. En ambos casos, estas revisiones y evaluaciones serán realizadas en las sesiones del Comité de Seguridad de la Información.

6. DIFUSIÓN

La presente Política será difundida por medio de su publicación en la sección “Seguridad de la Información” de la intranet institucional.

7. DEFINICIONES

- 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.

8. POLITICA

8.1 Organización Interna

Con el objetivo de establecer un marco de administración para iniciar y controlar la implementación y operación de la Seguridad de la Información dentro de la institución, el IND designa a un Encargado de Seguridad de la Información, conforma un Comité de Seguridad de la Información y aprueba una Política General de Seguridad de la Información que expresa adecuadamente el compromiso del Jefe de Servicio.



POLITICA DE LA ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN SISTEMA DE SEGURIDAD DE LA INFORMACIÓN

Página: Página 4 de 6

Versión : 2.0

Fecha Aprobación : 16 de mayo de 2019

Código: IND-SSI-A06-POL-01

8.1.1 Roles y responsabilidades de la Seguridad de la Información

Se debe definir y asignar todas las responsabilidades de Seguridad de la Información y Ciberseguridad dentro del IND, de acuerdo a las políticas de seguridad existentes. Para ello se debe considerar lo siguiente:

- Identificar las responsabilidades para la protección de activos individuales y para realizar procesos de Seguridad de la Información y Ciberseguridad, según corresponda.
- Definir las responsabilidades para las actividades de administración de riesgos de Seguridad de la Información y Ciberseguridad.
- Definir las responsabilidades en la protección de activos para realizar procesos de Seguridad de la Información y Ciberseguridad.

Las personas asignadas con responsabilidades de Seguridad de la Información y Ciberseguridad pueden delegar las tareas a otros, sin embargo siguen siendo responsables y deben verificar que cualquier tarea delegada se haya realizado correctamente.

8.1.2 Segregación de deberes

Se deben segregar los deberes y áreas de responsabilidad en conflicto en los sistemas de información, para reducir las oportunidades de modificación o uso indebido, no autorizado o no intencional de los activos de información institucionales.

Los derechos de acceso a los sistemas de información deben ser asignados a perfiles individuales, de forma tal que, las acciones realizadas con los accesos otorgados, sean de responsabilidad directa del funcionario.

El otorgamiento de accesos a los sistemas de información respecto a recursos de información del IND debe considerar una adecuada segregación de funciones, de modo que un mismo funcionario no pueda disponer, por su voluntad, del control de un proceso de negocios completo.

Las excepciones a la regla anterior deben ser aprobadas por la Jefatura correspondiente y autorizadas por la Jefatura del Departamento de Informática.



POLITICA DE LA ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN SISTEMA DE SEGURIDAD DE LA INFORMACIÓN

Página: Página 5 de 6

Versión : 2.0

Fecha Aprobación : 16 de mayo de 2019

Código: IND-SSI-A06-POL-01

8.1.3 Contacto con las autoridades

Con el objetivo de apoyar a la administración de incidentes de seguridad en el IND, se deben establecer procedimientos que especifiquen cuándo y a qué autoridades se debe contactar y cómo se debe informar los incidentes de seguridad de la información y de ciberseguridad.

Los contactos con otras autoridades incluyen a los proveedores de servicios básicos, servicios de emergencia, compañías de bomberos, Carabineros, Policía de Investigaciones y proveedores de telecomunicaciones, entre otros, según sea la naturaleza y/o severidad del incidente.

8.1.4 Contacto con grupos de interés especial

Para mantener actualizada la información que apoye el correcto desarrollo del SGSI y de la ciberseguridad, es necesario que la Institución mantenga contacto permanente con grupos o foros especializados y asociaciones profesionales. Asimismo esta información debería servir para mejorar el conocimiento sobre las nuevas prácticas, recibir alertas tempranas de avisos y parches relacionados con los ataques y vulnerabilidades y compartir e intercambiar información sobre las nuevas tecnologías, productos, amenazas y vulnerabilidades, entre otras temáticas relacionadas.

8.2 Teletrabajo

El IND permite el trabajo a distancia en casos específicos, con la debida justificación y autorización de la Jefatura del Departamento de Informática. La habilitación de VPN será por tiempo definido, el cual no podrá superar las 48 horas.

Para aquellos usuarios autorizados a trabajar de manera remota, se requiere que cumplan las siguientes condiciones:

- Velar por la seguridad física del espacio en que realice sus funciones, considerando la amenaza del acceso no autorizado a la información o a los recursos de parte de otras personas que utilizan el recinto (familia, amistades).
- No está permitido utilizar equipamiento propio, el trabajo deberá ser realizado utilizando el equipamiento entregado por el IND para esos fines.
- Al utilizar redes domésticas, éstas deben ser propias, no compartidas por terceros. Asimismo debe cerciorarse de que la configuración de la red cumpla con los requisitos de seguridad mínimos (claves robustas, acceso de usuario restringido).



**POLITICA DE LA ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN
SISTEMA DE SEGURIDAD DE LA INFORMACIÓN**

Página: Página 6 de 6

Versión : 2.0

Fecha Aprobación : 16 de mayo de 2019

Código: IND-SSI-A06-POL-01

- Cumplir con toda la normativa de seguridad que rige a la institución.

Aprobaciones

	Nombre	Cargo	Firma
Responsable de Elaboración	Cristian Villalobos Zamora	Encargado PMG Seguridad de la Información	
Responsable de Revisión y Aprobación	Jaime Bustos Brito	Encargado de Ciberseguridad	
Responsable de Revisión y Aprobación	Carola Molina Cecchi	Encargada de Seguridad de la Información	

Control de Cambios

Versión	Fecha	Responsable	Descripción
Versión 0.0	22-06-2017	Cristian Villalobos Z.	Se elabora esta primera versión del presente documento para dar cumplimiento al PMG-SSI 2017 y abordar requerimientos internos del IND.
Versión 1.0	02-07-2018	Cristian Villalobos Z.	Se modifica la difusión de la política.
Versión 2.0	16-05-2019	Cristian Villalobos Z.	Se incluye ciberseguridad en el objetivo y contenido de la política.