



## **POLITICA DE RECURSOS HUMANOS SISTEMA DE SEGURIDAD DE LA INFORMACIÓN**

Página: Página 1 de 5

Versión : 2.0

Fecha Aprobación : 16 de mayo de 2019

Código: IND-SSI-A07-POL-01

### **1. OBJETIVO**

Contar con una Política que permita asegurar que los funcionarios y personal externo conozcan, comprendan y cumplan correctamente sus responsabilidades en materias de Seguridad de la Información y Ciberseguridad, según sea pertinente para su función laboral.

### **2. ALCANCE**

Esta política aplica a todos los funcionarios, independiente de su calidad contractual, del Instituto Nacional de Deportes (IND), incluido el personal externo, que participan directa o indirectamente en los procesos de provisión que sustentan los productos estratégicos del IND, de acuerdo a lo establecido en el Formulario de Definiciones estratégicas (A1).

### **3. MATERIAS ESPECIFICAS QUE ABORDA**

- A.07.01.01 Selección
- A.07.01.02 Términos y condiciones de empleo
- A.07.02.01 Responsabilidades de la dirección
- A.07.02.02 Concientización, educación y capacitación sobre la seguridad de la información
- A.07.02.03 Proceso disciplinario
- A.07.03.01 Despido o cambio de responsabilidades en el empleo

### **4. ROLES Y RESPONSABILIDADES**

- **Comité de Seguridad de la Información:**
  - Ser responsable del cumplimiento, ciclo de vida y actualización de la presente Política.
  - Velar por la correcta implementación de los controles de seguridad mencionados en la presente política.
- **Encargado/a de Seguridad de la Información:**
  - Asesorar al Departamento de las Personas en materias de Seguridad de la Información.
  - Monitorear el avance general de la implementación de las estrategias de control y tratamiento de los riesgos asociados a la Seguridad de la Información.
  - Velar por el correcto cumplimiento de la presente política.



## POLITICA DE RECURSOS HUMANOS SISTEMA DE SEGURIDAD DE LA INFORMACIÓN

Página: Página 2 de 5

Versión : 2.0

Fecha Aprobación : 16 de mayo de 2019

Código: IND-SSI-A07-POL-01

- **Encargado/a de Ciberseguridad**
  - Apoyar el proceso de sensibilización en materias de Ciberseguridad al interior de la Institución.
  
- **Departamento de la Personas:**
  - Definir, gestionar y supervisar los procesos y procedimientos de selección, reclutamiento, contratación y desvinculación de todos los funcionarios.
  - Definir, gestionar e implementar los planes anuales de capacitación e inducción de los funcionarios en las temáticas de Seguridad de la Información y Ciberseguridad.
  
- **Jefaturas de Área:**
  - Definir los perfiles, requisitos, responsabilidades y necesidades de capacitación de los distintos cargos de su área.

### 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.
- **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.



## **POLITICA DE RECURSOS HUMANOS SISTEMA DE SEGURIDAD DE LA INFORMACIÓN**

Página: Página 3 de 5

Versión : 2.0

Fecha Aprobación : 16 de mayo de 2019

Código: IND-SSI-A07-POL-01

### **8. POLITICA**

#### **8.1 Verificación de antecedentes**

- Todo proceso de Reclutamiento y Selección de Personal debe ser canalizado sólo a través del Departamento de las Personas.
- El personal del Departamento de las Personas es el responsable de verificar los antecedentes personales, laborales y académicos del postulante, y en general, cualquier otro tipo de antecedente que pudiera afectar la Seguridad de la Información y/o a la Ciberseguridad, al interior de la institución.
- Cuando se contrata a una persona para un rol específico de Seguridad de la Información y/o de Ciberseguridad, se debe asegurar que el postulante cuente con las competencias necesarias para desempeñar el rol y que pueda ser confiable.
- Donde un trabajo, ya sea de empleo inicial o por cambios de funciones, requiera que la persona tenga acceso a las instalaciones de procesamiento de información y, en particular si se maneja información sensible, también se deben considerar más verificaciones en mayor detalle.

#### **8.2 Términos y condiciones de empleo**

Los roles y responsabilidades de Seguridad de la Información y Ciberseguridad deben aparecer en los perfiles de cargo publicados, de manera que sea conocidos por los postulantes al trabajo durante el proceso previo al empleo.

Todos los funcionarios de la institución, independiente de su calidad contractual, deberán:

- Cumplir la normativa de Seguridad de la Información existente en la institución.
- Cumplir a cabalidad lo establecido en la letra h, Artículo 55, TITULO III del Estatuto Administrativo que detalla dentro de las obligaciones de los funcionarios, “Guardar secreto en los asuntos que revistan el carácter de reservados en virtud de la ley, del reglamento, de su naturaleza o por instrucciones especiales”.

#### **8.3 Responsabilidades de la dirección**

La institución pone a disposición de los funcionarios, diversos recursos e instancias para que conozcan y cumplan sus responsabilidades de Seguridad de la Información y Ciberseguridad. La dirección apoya y respalda toda la normativa de Seguridad de la Información desarrollada en el servicio, mediante la aprobación de una Política General de Seguridad de la Información.



## **POLITICA DE RECURSOS HUMANOS SISTEMA DE SEGURIDAD DE LA INFORMACIÓN**

Página: Página 4 de 5

Versión : 2.0

Fecha Aprobación : 16 de mayo de 2019

Código: IND-SSI-A07-POL-01

### **8.4 Concientización, educación y capacitación sobre la seguridad de la información**

Todos los funcionarios deben recibir educación y capacitación regulares sobre las políticas y procedimientos de Seguridad de la Información, así como sobre las temáticas de Ciberseguridad, según sea pertinente para sus funciones.

Para ello el Departamento de la Personas debe incluir en sus planes de capacitación e inducción, las temáticas relacionadas con la Seguridad de la Información y Ciberseguridad, de manera que los funcionarios conozcan sus responsabilidades, considerando la información institucional que se va proteger y los controles que se han implementado para ello.

El programa de concientización también se debe actualizar de manera regular para que esté de acuerdo con las políticas y procedimientos vigentes en el IND, considerando las lecciones aprendidas de los incidentes de Seguridad de la Información y/o Ciberseguridad según corresponda.

### **8.5 Proceso disciplinario**

El no cumplimiento de la normativa interna de la institución, así como la vulneración de la confidencialidad, integridad o disponibilidad de los activos de la información institucionales, podrán dar paso a un proceso disciplinario cuyo resultado determinará las sanciones aplicables.

### **8.6 Despido o cambio de responsabilidad en el empleo**

Las responsabilidades y deberes de confidencialidad y no divulgación de la información sensible de la institución a la que tengan acceso los funcionarios, contratistas y/o proveedores, continuaran por tiempo indefinido una vez que la relación laboral haya llegado a su término. Esto deberá quedar establecido al momento de la contratación.



## POLITICA DE RECURSOS HUMANOS SISTEMA DE SEGURIDAD DE LA INFORMACIÓN

Página: Página 5 de 5

Versión : 2.0

Fecha Aprobación : 16 de mayo de 2019

Código: IND-SSI-A07-POL-01

### 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 0.1	04-08-2017	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.