1. OBJETIVO

El objetivo de la presente Política es evitar el acceso no autorizado a la información y a los sistemas de información (correo electrónico institucional, software, aplicaciones, carpetas compartidas, etc.) del Instituto Nacional de Deportes (IND), mediante la instalación de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma NCh-ISO 27001:2013, con foco en Ciberseguridad, asegurando la continuidad de los servicios críticos del IND 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. Aplica también a todos los sistemas, bases de datos, software, etc., que den soporte a todos los procesos de provisión institucionales definidos en la Ficha de Definiciones Estratégicas (A1).

3. MATERIAS ESPECIFICAS QUE ABORDA

La presente Política está asociada a los siguientes controles de la norma NCh-ISO 27001:2013:

- A.09.01.01 Política de control de accesos
- A.09.01.02 Control de acceso a las redes y servicios asociados
- A.09.02.01 Gestión de altas/bajas en el registro de usuarios
- A.09.02.02 Asignación de acceso de usuario
- A.09.02.03 Gestión de derechos de acceso privilegiados
- A.09.02.04 Gestión de información confidencial de autenticación de usuarios
- A.09.03.01 Uso de información confidencial para la autenticación
- A.09.04.01 Restricción del acceso a la información
- A.09.04.02 Procedimientos seguros de inicio de sesión
- A.09.04.03 Gestión de contraseñas de usuario
- A.09.04.04 Uso de programas utilitarios privilegiados
- A.09.04.05 Control de acceso al código fuente de los programas

4. ROLES Y RESPONSABILIDADES

- **Comité de Seguridad de la Información:** Supervisar la implementación de las actividades que se desprenden de la presente política.

- **Encargado/a de Seguridad de la Información:** Velar por el correcto cumplimiento de la presente política.
- **Jefatura Unidad de Coordinación Informática:** Disponer los controles y reglas de control de acceso a los sistemas de información según lo establecido en la presente política.
- **Área de Operaciones de Unidad de Coordinación Informática:** Gestionar los derechos de acceso a los medios de procesamiento de información que tenga a su cargo según lo establecido en la presente política.
- **Usuarios/as:** Son responsables de la información, equipos informáticos y de los servicios de red de la institución que sean puestos a su disposición, debiendo velar por el correcto cumplimiento de las normas ya señaladas, por ende, cualquier omisión voluntaria o involuntaria será sancionada en conformidad a la normativa vigente, según corresponda.

5. DIFUSIÓN

La forma de difusión de la presente Política será a través de su publicación en la sección "Seguridad de la Información" de la intranet institucional.

6. REVISIÓN Y EVALUACIÓN

La presente Política se debe revisar y evaluar su correcta aplicación cuando se cumpla un año de su aprobación y formalización o cada vez que se detecte un evento que propicie un ajuste de las declaraciones establecidas; en ambos casos, estas revisiones se realizaran en sesiones del Comité de Seguridad de la Información.

7. POLITICA

7.1 Cumplimiento de la legislación

Las medidas de control de acceso a los sistemas de información definidas se deben cumplir y ser consistentes con lo dispuesto por las normas y requerimientos legales definidos en la Política General de Seguridad de la Información.

7.2 Control de acceso a los sistemas de información

Todos/as los/as funcionarios/as del IND, incluso terceros, deben tener acceso sólo a la información que necesitan para el desarrollo legítimo de sus funciones y actividades dentro de la institución. La asignación de privilegios y acceso a los activos de información (correo

electrónico institucional, software, aplicaciones, carpetas compartidas, etc.) deben estar basados en las necesidades de las áreas y aprobados por el/la propietario/a de los activos.

Estas necesidades de acceso deben ser determinadas por las respectivas jefaturas, en función de las tareas asignadas al cargo del/la funcionario/a.

Para todo medio de procesamiento de información al que se necesite conceder accesos (por ejemplo: servidores, aplicaciones, carpetas compartidas, base de datos, etc.), el/la dueño/a de la información en conjunto con la Unidad de Coordinación Informática debe asignar un/a responsable del medio, quién será encargado/a de autorizar los permisos de acceso y solicitar los espacios necesarios.

Sólo se deben conceder accesos a externos a la institución previa solicitud del/la dueño/a del medio de procesamiento de información y el/la dueño/a de la información. Las cuentas de acceso a terceros deben tener especificado un tiempo de expiración, el que debe ser controlado por el Área de Operaciones de la Unidad de Coordinación Informática, según corresponda.

El Comité de Seguridad de la Información del IND tiene la facultad de suspender o eliminar los accesos a cualquier persona que represente riesgo para la confidencialidad, integridad o disponibilidad de la información cuando se detecte o reporte un incidente relacionado a la seguridad de la información.

Cualquier intento de acceso no autorizado a los equipos, carpetas compartidas, sistemas e información será considerado un incidente grave, por lo que debe reportarse de inmediato según lo descrito en el procedimiento de Gestión de Incidentes de Seguridad de la Información.

8.3 Administración del acceso a los sistemas de información

La responsabilidad de solicitar un determinado perfil de acceso a los sistemas de información a un/a usuario/a, corresponderá a la Jefatura directa.

La responsabilidad de gestionar los accesos solicitados de usuario/a en las aplicaciones radica en la Unidad de Coordinación de Informática.

No se podrá otorgar el acceso a los sistemas de información a ningún/a usuario/a hasta que se haya completado el proceso de autorización y registro realizado por la Unidad de Coordinación de Informática.

8.4 Administración de accesos especiales

El otorgamiento de accesos a los sistemas de información con mayores privilegios (por ejemplo acceso a: bases de datos, código fuente, etc.) a funcionarios/as que no pertenezcan a la Unidad de Coordinación de Informática, debe ser solicitado por la Jefatura correspondiente o quién delegue, al Encargado/a de Seguridad de la Información justificando dicha solicitud.

8.5 Segregación de funciones

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 la Unidad de Coordinación de Informática.

8.6 Revisión de los derechos de acceso

El Área de Operaciones de la Unidad de Coordinación de Informática, es responsable de los accesos a los distintos sistemas de información, de tal forma que se establezca un control efectivo desde el registro inicial de la cuenta hasta el momento en que requiera ser modificada, revocada o eliminada.

Los derechos de accesos deben ser revisados por el Área de Operaciones de la Unidad de Coordinación de Informática:

- A intervalos regulares no mayores a 6 meses.
- Después de cualquier cambio mayor en la institución.
- Los accesos de cuentas con mayores privilegios, deben ser revisados al menos 2 veces al año.

8.7 Revocación de los accesos

Es responsabilidad de las Jefaturas Directas informar formalmente las desvinculaciones de y/o cambios que presente los/as usuarios/as.

Ante una situación de un cambio de cargo de un/a funcionario/a, se deben revisar sus permisos de acceso asignados y verificar que éstos sigan siendo válidos de acuerdo a su nueva función.

Cuando un/a funcionario/a termina su relación laboral con el IND, todos sus permisos de acceso a la información deben ser revocados.

7.8 Tele-Trabajo

Cualquier funcionario/a del IND, solicitado por la jefatura directa y autorizado por la jefatura de la Unidad de Coordinación Informática, que requiera tener acceso a la información de la institución desde redes externas y fuera del horario de trabajo, podrá acceder remotamente mediante un proceso de autenticación, mediante el uso de conexiones seguras y velando por el cumplimiento de requisitos de seguridad de los equipos desde los que se accede, considerando además lo establecido en la "*Política de la Organización de la Seguridad de la Información*", en el punto que trata sobre *Trabajo Remoto*.

7.9 Uso de programas utilitarios privilegiados

La instalación de software en estaciones es sólo labor y responsabilidad del Área de Operaciones de la Unidad de Coordinación Informática, aplicando para los usuarios el principio de menor privilegio y privilegio de restringido, restringiendo el uso de programas utilitarios privilegiados que pueden ser capaces de anular el sistema. Para esto se considerarán los siguientes controles en las estaciones de trabajo del personal del IND:

- Uso de procedimientos de identificación, autenticación y autorización para los programas utilitarios privilegiados.
- Segregación en el uso de programas utilitarios privilegiados, sólo a aquellos usuarios administradores debidamente identificados.
- Limitación del uso de programas utilitarios privilegiados al número mínimo práctico de usuarios identificados y autorizados.
- Autorización para programas utilitarios privilegiados, permitidos en el IND.
- Limitación de la disponibilidad de programas utilitarios privilegiados, es decir, por la duración de un cambio autorizado.
- Registro de todo el uso de los programas utilitarios privilegiados
- Definición y documentación de los niveles de autorización para los programas utilitarios privilegiados.
- Eliminación o deshabilitación de todos los programas utilitarios privilegiados.
- No dejar los programas utilitarios privilegiados disponibles a los usuarios que tienen acceso a las aplicaciones de los sistemas donde se requiere la segregación de deberes.

7.10 Control de Acceso al código fuente de los programas

El acceso al código de fuente de programas y los elementos asociados (como diseños, especificaciones, planes de verificación y validación) se controlarán estrictamente a través de sistemas dispuestos para estos efectos, de manera de evitar la introducción de funcionalidades no autorizadas y para evitar los cambios no intencionales, así como también, para mantener la confidencialidad de la propiedad intelectual. Para lograr este objetivo, se implementarán las siguientes reglas:

- Las bibliotecas de fuente de programas se mantendrán en sistemas operacionales, dispuestos para estos efectos.
- El código de fuente de programas y las bibliotecas de fuente de programas se administrarán de acuerdo a los procedimientos establecidos de desarrollo de software al interior del IND.
- El personal de apoyo no contará con acceso sin restricción a las bibliotecas de fuente de programas.
- La actualización de las bibliotecas de fuente de programas y los elementos asociados, junto con la emisión de las fuentes de programas a los programadores solo se realizará cuando se haya recibido la autorización correspondiente, de acuerdo a los procedimientos establecidos.
- Las listas de programas se mantendrán en un entorno seguro, a través de los sistemas dispuestos para estos efectos.
- Se mantendrá un registro de auditoría de todos los accesos a las bibliotecas de fuente de programas.
- El mantenimiento y el copiado de bibliotecas de fuente de programas estarán sujetos a procedimientos de control de cambios estrictos, de acuerdo a los procedimientos establecidos en el Instituto.

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	06-10-2016	Cristian Villalobos Z.	Se elabora esta primera versión del presente documento.
Versión 1.0	02-07-2018	Cristian Villalobos Z.	Se modifica el formato, la difusión de la política y las responsabilidades.
Versión 2.0	16-05-2019	Cristian Villalobos Z.	Se incluye ciberseguridad en el objetivo y contenido de la política.