1. OBJETIVO

Evitar accesos físicos no autorizados, daños e interferencias a los activos de información y a las instalaciones de procesamiento de información del Instituto Nacional de Deportes (IND) , de acuerdo a la norma NCh-ISO 27001:2013, de manera de resguardar la confidencialidad, integridad y disponibilidad de la información.

2. ALCANCE

La presente política aplica a todas las oficinas y dependencias de la institución, ubicadas en Fidel Oteiza 1956 pisos 3 y 4 y a las instalaciones de procesamiento de información ubicadas en Avenida Grecia N° 2001, Ñuñoa, lugar donde se almacena y procesa la información vinculada a los procesos de provisión vigentes en el IND, que dan soporte a los productos estrátegicos institucionales, de acuerdo a lo establecido en la Ficha de Definiciones estratégicas (A1).

3. MATERIAS ESPECÍFICAS QUE ABORDA

- A.11.01.01 Perímetro de seguridad física
- A.11.01.02 Controles de acceso físico
- A.11.01.03 Seguridad de oficinas, salas e instalaciones
- A.11.01.04 Protección contra amenazas externas y del ambiente
- A.11.01.05 Trabajo en áreas seguras
- A.11.01.06 Áreas de entrega y carga
- A.11.02.01 Ubicación y protección del equipamiento
- A.11.02.02 Elementos de soporte
- A.11.02.04 Mantenimiento del equipamiento
- A.11.02.05 Retiro de activos
- A.11.02.06 Seguridad del equipamiento y los activos fuera de las instalaciones
- A.11.02.07 Seguridad en la reutilización o descarte de equipos
- A.11.02.08 Equipo de usuario desatendido
- A.11.02.09 Política de escritorio y pantalla limpios

4. ROLES Y RESPONSABILIDADES

- Comité de Seguridad de la Información:
  - Ser responsable del cumplimiento, ciclo de vida y actualización de la presente Política de Seguridad Física y Ambiental del IND.
  - Velar por la correcta implementación de los controles de seguridad mencionados en la presente política.

- Encargado/a de Seguridad de la Información:
  - Asesorar al Jefe de Servicio 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 presente política.

- Unidad de Administración:
  - Proveer y gestionar los dispositivos y mecanismos de control de acceso físico a las dependencias e instalaciones de procesamiento de información del IND.
  - Gestionar las claves de los dispositivos de control de acceso físico.

- Unidad Coordinación de Informática:
  - Definir los requisitos de seguridad del Datacenter.
  - Autorizar y supervisar el acceso al Datacenter.
  - Aplicar las políticas y procedimientos de seguridad física del Datacenter.

- Departamento de Gestión de Personas:
  - Gestionar las nuevas incorporaciones y desvinculaciones de funcionarios.

- Comité Paritario de Higiene y Seguridad:
  - Desarrollar, implementar y mantener planes de seguridad para las dependencias e instalaciones del IND.

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 debe ser difundida por medio de su publicación en la sección "Seguridad de la Información" de la intranet institucional.

7. DEFINICIONES

- **Datacenter:** Es aquel espacio o habitación donde se concentran los recursos tanto de hardware y software necesarios para el procesamiento de la información de una organización.
- **Perímetro de Seguridad Física:** Está constituida por la zona cercada por los elementos físicos que en conjunto permiten diferenciar las instalaciones del servicio respecto del exterior, como paredes, pertas, accesos, salidas y entradas, protegidos con dispositivos de control de acceso magnético o biométrico, o un puesto manual de recepción.
- **Área Segura:** Son áreas que contienen información sensible o crítica y las instalaciones de procesamiento de información. Como por ejemplo salas de servidores, Datacenter u Oficina de Partes.
- **Área restringida:** Son aquellas áreas cuyo acceso o movimiento dentro de las mismas está sujeto a ciertas restricciones o medidas de control especial por razones de seguridad. Se establecen con el propósito de resguardar los bienes, materiales, información y/o actividades que allí se encuentran o desarrollan. Dentro de las áreas establecidas como restringidas se encuentran las oficinas de directores, bodegas de almacenamiento de activos y existencias y oficinas de informática.
- **Equipos Críticos:** Son aquellos equipos que dan soporte a las operaciones críticas del servicio, tales como: servidores, dispositivos de comunicaciones, de seguridad y servicio básicos de apoyo.

8. POLITICA

8.1 Áreas Seguras

8.1.1 Perímetros de seguridad física

- Se deben definir perímetros de seguridad de acuerdo a los requisitos de seguridad de los activos dentro del perímetro y los resultados de una evaluación de riesgos.
- El sitio donde se albergan las instalaciones de procesamiento de información (Datacenter) debe ser físicamente sólido; el techo exterior, las paredes y el piso del sitio deben ser de construcción sólida y todas las puertas externas deben estar protegidas adecuadamente contra el acceso no autorizado con algún mecanismo de control efectivo; las puertas y ventanas se deben cerrar con llave correctamente cuando se dejan sin vigilancia y se debe

considerar una protección externa para las ventanas, en particular si se ubican a nivel del suelo.

- Se debe contar con un área de recepción atendida por una persona u otros medios efectivos para controlar el acceso físico a los pisos que el IND ocupa dentro del edificio; el acceso se debe restringir solo al personal autorizado y tomar las medidas correspondientes para el acceso de visitas o personal ajeno al IND.
- Se deben utilizar barreras físicas donde corresponda para evitar el acceso físico no autorizado y la contaminación ambiental.

8.1.2 Controles físicos de entrada

- Las áreas seguras deben estar protegidas con controles de entrada adecuadas para garantizar que sólo se permita el acceso al personal autorizado.
- Se debe registrar en una bitácora la fecha, la hora de entrada y salida de las visitas previamente autorizadas. Solo se debe otorgar acceso para propósitos específicos y autorizados de acuerdo a las instrucciones de los requisitos de seguridad del área. Se debe autenticar la identidad de las visitas con un medio adecuado.
- Todos los funcionarios, visitas y partes externas que por algún motivo especifico deban circular por una zona segura o restringida deben portar algún tipo de identificación visible y se debe notificar inmediatamente al Encargado de Seguridad si se encuentra a cualquier persona desconocida que no porte una identificación visible.
- El acceso al Datacenter se debe permitir solo a personas autorizadas mediante la implementación de controles de acceso adecuados.
- Está prohibido el acceso a funcionarios no autorizados a aquellas áreas declaradas como seguras o restringidas.
- El personal de aseo debe estar identificado con su uniforme de la empresa mientras desarrollen sus labores.
- Se debe otorgar acceso restringido a los proveedores a las áreas seguras sólo cuando sea necesario. Este acceso se debe autorizar y monitorear.
- Los derechos de acceso a las áreas seguras se deben revisar y actualizar de manera regular y revocar cuando sea necesario.

8.1.3 Protección de oficinas, salas e instalaciones

- Las áreas seguras se deben emplazar de manera de evitar el acceso del público.
- La ubicación de las áreas seguras no deben ser anunciadas mediante signos o señales en áreas de acceso público.

- Las instalaciones se deben configurar de manera de evitar que la información o las actividades confidenciales se vean y/o escuchen desde fuera.
- Los directorios y libretas telefónicas internas que identifican la ubicación de las instalaciones de procesamiento de información confidencial no deben estar disponibles fácilmente a personas no autorizadas.

8.1.4 Protección contra las amenazas externas o ambientales

- Se debe diseñar y aplicar una protección física contra desastres naturales, ataques maliciosos o accidentes.
- Debe existir un plan de evacuación y/o de emergencia del personal cuando sea necesario y para la protección de los activos de información críticos en caso de emergencia.

8.1.5 Trabajo en áreas seguras

- El personal debe estar al tanto de la existencia de las áreas seguras y de las actividades dentro de ellas, según se considere necesario. Esto debe ser informado en el proceso de inducción de cada funcionario según sean sus labores.
- No está permitido el trabajo de terceros no supervisado en áreas seguras, tanto por motivos de seguridad como para evitar las oportunidades de actividades maliciosas.
- No están permitidos los equipos fotográficos, de video o audio, como las cámaras de dispositivos, dentro de las áreas seguras, a menos que sean expresamente autorizadas por el responsable a cargo.

8.1.6 Áreas de carga y descarga

Se deben controlar los puntos de acceso como las áreas de entrega y carga y otros puntos donde pudieran ingresar personas no autorizadas a las instalaciones seguras, considerando lo siguiente:

- El acceso al área de entrega y carga desde fuera del edificio está permitido solo al personal identificado y previamente autorizado.
- El área de entrega y carga debe estar diseñado de manera que se puedan cargar y descargar los suministros sin el que el personal que realiza la entrega acceda a otras áreas del edificio.
- Las puertas externas a un área de entrega y carga se deben resguardar cuando se abren las puertas internas.
- El material entrante se debe registrar de acuerdo con los procedimientos de administración de activos en la entrada al sitio.

- Se debe inspeccionar el material entrante en busca de evidencias de manipulación indebida en la ruta. Si se descubre algún indicio de manipulación indebida o adulteración del contenido y/o empaque del material, se debe informar inmediatamente al Encargado de Seguridad.

8.2 Equipos

8.2.1 Emplazamiento y protección de equipos

Los equipos se deben emplazar y proteger para reducir los riesgos de las amenazas ambientales y las oportunidades de acceso no autorizado, considerando lo siguiente:

- Los equipos se deben emplazar en un lugar determinado para minimizar el acceso innecesario a las áreas de trabajo.
- Se deben adoptar controles para minimizar el riesgo de posibles amenazas físicas y ambientales, es decir, robos, incendios, humo, agua, polvo, vibraciones, efectos químicos, interferencia del suministro eléctrico, interferencia en las comunicaciones, radiación electromagnética y vandalismo.
- Las instalaciones de procesamiento de información que manejan datos sensibles deben estar ubicados de manera estratégica para reducir el riesgo de acceso de personas no autorizadas.
- Está prohibido comer, beber y/o fumar en la proximidad o dentro de las instalaciones de procesamiento de información.
- Se deben monitorear las condiciones ambientales como la temperatura y la humedad de manera de evitar que éstas puedan afectar adversamente a la operación de las instalaciones de procesamiento de información y en las áreas seguras.

8.2.2 Servicios básicos de suministro

Los equipos críticos deben estar protegidos contra cortes de luz y otras interrupciones provocadas por fallas en los servicios básicos de suministro (electricidad, telecomunicaciones, suministro de agua, gas, ventilación y aire acondicionado).

En el Datacenter debe existir iluminación y comunicaciones de emergencia. Los interruptores de emergencia y los switches para cortar la electricidad, el agua, el gas u otros servicios básicos deben estar ubicados cerca de las salidas de emergencia o de las salas equipadas.

Los servicios básicos de suministro deben cumplir con los siguientes requerimientos:

- Deben cumplir con las especificaciones del fabricante del equipo y con los requisitos legales locales.
- Deben someterse a evaluaciones periódicas para cumplir con el crecimiento del servicio y las interacciones con otros servicios básicos.

- Deben someterse a inspecciones y pruebas regularmente para garantizar su correcto funcionamiento.

8.2.3 Mantención de equipos

Los equipos críticos se deben mantener correctamente para garantizar su disponibilidad e integridad continua.

Se deben considerar las siguientes pautas para mantención de los equipos críticos:

- Las mantenciones de los equipos se deben realizar de acuerdo a los intervalos y especificaciones de servicio recomendados por el proveedor.
- Solo el personal autorizado debe realizar reparaciones y labores de mantenimiento y servicio a los equipos.
- Se deben mantener registros de todas las fallas y mantenciones preventivas y correctivas.
- Se deben implementar controles adecuados cuando se programa la mantención de equipos, considerando si ésta la realizará personal externo a la organización; donde sea necesario se debe eliminar la información confidencial del equipo, o bien la debería realizar personal interno de soporte.
- Una vez realizada la mantención de un equipo, luego de volver al funcionamiento, el equipo debe ser inspeccionado para garantizar que no ha sido adulterado y que funciona adecuadamente.

8.2.4 Eliminación o reutilización segura de equipos

Antes de dar de baja un equipo se debe eliminar, destruir o sobrescribir toda la información y software licenciado que éste contenga, utilizando técnicas que impidan la recuperación de la información en lugar de recurrir al borrado tradicional del equipo.

En el caso de la reutilización de equipos, se debe verificar la eliminación de toda aquella información que no debería tener acceso el nuevo usuario.

Se debe considerar que además del borrado seguro del disco, el cifrado del disco completo reduce el riesgo de divulgar información confidencial cuando se elimina o vuelve a implementar el equipo, siempre que:

- El proceso de cifrado sea lo suficientemente fuerte y que cubra a todo el disco (incluido el espacio despejado, los archivos de intercambio, etc.).
- Las claves de cifrado sean lo suficientemente largas como para resistir los ataques de fuerza bruta.

- Las claves de cifrado en sí se mantengan de manera confidencial (es decir, que nunca se almacenen en el mismo disco).

8.2.5 Retiro de equipos

Los equipos no deben ser retirados fuera de la institución sin la autorización correspondiente, considerando lo siguiente:

- La Jefa de informática es quien autoriza el retiro de equipos fuera de las dependencias del IND, entendiéndose con ellos los computadores de escritorio, servidores y equipo de infraestructura.
- Este equipamiento debe ser previamente identificado antes de su salida, debiendo dejar un registro de la fecha y hora de salida, tiempo en que estará fuera, motivo de la salida y persona a cargo.
- Los notebooks que están asignados a los funcionarios pueden ser retirados de las dependencias del IND, siendo total responsabilidad de ellos el buen uso y protección de los mismos.

8.2.6 Seguridad de los equipos y los activos fuera de las dependencias

Al utilizar un equipo computacional (Notebook) o teléfonos móviles fuera de las instalaciones del IND, el usuario deberá considerar las siguientes pautas de protección del equipo:

- Nunca dejar sin supervisión el equipo.
- Observar y cumplir las instrucciones del fabricante en cuanto a la protección contra la exposición a campos electromagnéticos fuertes.
- En caso de utilizar sitios temporales de trabajo, el usuario debe velar por cumplir la misma normativa de seguridad que rige en la institución, es decir, documentos guardados bajo llave, escritorio despejado, controles de acceso para el equipo computacional y vías de comunicación segura.

8.2.7 Equipo de usuario desatendido

Los usuarios deben asegurase de que los equipos no supervisados cuentan con la protección adecuada de manera de poder evitar el acceso indebido a sistemas y/o información contenida en él.

Si por alguna razón no funciona el bloqueo automático del equipo, el usuario deberá cerrar sus sesiones activas. Se deben también cerrar las sesiones en los distintos sistemas, aplicaciones y/o servicios de redes cuando ya no se necesiten.

8.2.8 Política de escritorio despejado y pantalla despejada

- La información sensible o crítica para la institución que esté almacenada en medios electrónicos o papel, debe mantenerse guardada bajo llave cuando no se necesite, especialmente cuando la oficina esté desocupada.
- Los computadores deben estar protegidos con un mecanismo de bloqueo de pantalla y teclado mediante una contraseña, token o mecanismo de autenticación.
- Se debe controlar el uso no autorizado de fotocopiadoras u otro tipo de tecnologías de reproducción (es decir, escáneres, cámaras digitales).
- Los documentos que contengan información sensible o clasificada se deben extraer de las impresoras inmediatamente.

Aprobaciones

	Nombre	Cargo	Firma
Responsable de Elaboración	Cristian Villalobos Zamora	Encargado PMG Seguridad de la Información	
Responsable de Revisión	Edson Maya Vera	Encargado Área de Operaciones	
Responsable de Revisión y Aprobación	Carola Molina Cecchi	Encargada de Seguridad de la Información	

Control de Cambios

Versión	Fecha	Responsable	Descripción
Versión 1.0	18-07-2017	Cristian Villalobos Z.	Se elabora esta primera versión del presente documento para dar cumplimento al PMG-SSI 2017 y abordar requerimientos internos del IND.
Versión 2.0	02-07-2018	Cristian Villalobos Z.	Se modifica la difusión de la política y las responsabilidades